LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för Informatik

Det Smarta Hemmet

Användarnas förtroende för de smarta enheterna i hemmet

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Emilia Petersson
Therése Sördal

Handledare: Miranda Kajtazi

Examinatorer: Magnus Wärja
Björn Svensson

Det Smarta Hemmet: Användarnas förtroende för de smarta enheterna i hemmet

FÖRFATTARE: Emilia Petersson och Therése Sördal

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

FRAMLAGD: Maj, 2018

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 177

NYCKELORD: Smarta hem, data analytics, personlig integritet, informatik, datahantering

SAMMANFATTNING:
Tack vare nytänkande teknik och den tekniska utvecklingen, har en kombination av Cloud Computing, Internet of Things och Data Analytics kunnat realisera fenomenet smarta hem. Med syfte om att underlätta hushållens vardag genom diverse smarta enheter har tekniken med ständigt internetanslutna enheter i hushållen som hanterar känslig och personligt identifierbar data, har dock orosmoln kring den personliga integriteten väckts. Som ett resultat av den intensivt växande marknaden av smarta hem ökar även mängden data som samlas in från individer, vilket i sin tur kan medföra en potentiell ökning av det globala flödet av Big Data. Genom en kvalitativ studie, undersöker vi vad som krävs för att de smarta enheterna ska upplevas pålitliga ur användarens perspektiv. I slutet av uppsatsen presenteras akronymen MITT, vilken tagits fram av författarna genom att ställa CIA-triaden och Big Data's Dimensioner i perspektiv till det smarta hemmet. MITT, förväntas vara ett hjälpmedel för att tydliggöra vad som krävs av de smarta enheternas tillverkare, i arbetet mot att göra det smarta hemmets datahanteringen ännu mer pålitlig.

Innehåll

Figurförteckning

Tabellförteckning

Begrepp & Definitioner

BEGREPP	DEFINITION
Användare	Detta begrepp definieras av följande beskrivning genom hela uppsatsen: En person som använder sig av smarta enheter i hemmet.
CEH	Begreppet står för ”Certified Ethical Hacker”. Detta är en person som arbetar på professionell nivå med att förstå och hitta svagheter i system. Personen använder samma kunskap och verktyg som skadliga hackare, dock på ett lagligt och legitimt sätt för att bedöma och stärka ett systems säkerhet (EC-Council, n.d.).
Extensiv Studie	När en studie går på bredden (Jacobsen, 2002).
Intensiv Studie	När en studie går på djupet (Jacobsen, 2002).
IPAx	Intervjuperson Användare, x definierar vilken användare det är.
IPFR	Intervjuperson Företagsrepresentant.
IPSS	Intervjuperson Svensk Säkerhetsmyndighet.
Plagiera / Plagiat	Att plagiera innebär att författaren imiterar och skriver av någon annans text, utan att citera källan. Författaren använder texten som att den vore dens eget verk (Svenska Akademins Ordlista, n.d.).
SQL	SQL står för Structured Query Language och är ett standardiserat programmeringsspråk för att hämta och använda data i en databas (W3Schools, n.d.).
USD	Beteckning för amerikanska dollar, valutan för USA.

1. Introduktion

I introduktionen presenteras uppsatsens bakgrund, problemformulering, forskningsfråga, syfte samt avgränsningar.

1.1 Bakgrund

Idag samlas stora mängder data in från smarta byggnader (Statista, 2018a), vilken kan möjliggöra kartläggning av användare av smarta enheter i hemmet (Molina-Markham et al. 2010). Eftersom smarta hem är anslutna till ett nätverk, kan data enkelt delas mellan de smarta enheterna och externa partner. Något som kan ha godkänts av användaren genom accepterande av licensavtalen, men som däremot inte alltid framgår särskilt tydligt för användaren på grund av breda och fritolkande formuleringar.

Idag finns lagar och regler kring hur den personliga integriteten måste skyddas samt för utformande av säkerthetspolicyer. I dagens samhälle där Big Data, Internet of Things och Data Analytics frodas, verkar de dock inte alltid räcka till för att säkerställa den personliga integriteten (Bugeja, Jacobsson & Davidsson, 2016). Ju mer data som samlas in, desto mer data analyseras och desto mer känslig information skapas som i sin tur kan identifiera en specifik människa. Genom att analysera informationen kan det smarta hemmet i slutändan förutspå beteendemönster (Molina-Markham et al. 2010), något som kanske underlättar vardagen men samtidigt kan ha en negativ effekt för den personliga integriteten. Ur ett både etiskt och rättsligt perspektiv, ligger denna typ av datainsamling på en hårfin linje för huruvida det klassificeras som okej eller som ett intrång på den personliga integriteten (Birchley et al. 2017). Vad är det egentligen som indikerar pålitlighet? Väger verkligen effektivisering och underlättande av vardagliga handlingar tyngre än säkerheten av den personliga integriteten? Det är en fråga som idag är allt mer aktuell efter Facebook-Carmbridge Analytica skandalen.

Genom att det smarta hemmet består av en mängd nätverksuppkopplade enheter och system, som med hjälp av molntjänster kan lagra och hantera data i nätverket (Microsoft Azure n.d.a), ökar risken för att obehöriga personer får tillgång till data om enheten inte försetts med rätt säkerhetstekniker. Ett vanligt problem i dagens informations- och digitaliseringssamhälle är mängden identitetsstölder som förekommer på internet (Olsdotter-Arnmar & Näslund, 2013), något som det smarta hemmet kan bli en bidragande faktor till om insamlad data inte behandlas korrekt. Det är därför viktigt för såväl användare som tillverkare av smarta enheter att beakta konfidentialiteten, integriteten samt tillgängligheten för den data som hanteras. Molina-Markham et al. (2010) förklarar hur det krävs att användare är medvetna om vilken information som samlas in av de smarta enheterna, för att det de inte ska riskera säkerheten kring sin personliga integritet.

För att ett smart hem ska fungera optimalt, är det nödvändigt att samla in känslig och detaljerad data av dess användare. Samtidigt gäller det att de smarta enheterna inte samlar in mer data än vad som behövs för att utföra tjänsten, för att undvika integritetskränkning (Datainspektionen, 2012).

1.1.2 Tidigare forskning

Vid granskning av ett relevant forskningsområde, ämnade vi att hitta ett område som är aktuellt i tid och samtidigt, enligt vår uppfattning, i behov av vidareforskning. Fenomenet kring spridning av data i en industriell kontext är relativt komplext (Mair, 2018). Det smarta hemmets snabba tillväxt på marknaden (Statista, 2018b) gör dock ämnet väldigt aktuellt och påverkar individen mer än vad vissa användare orkar bry sig om idag (Quah & Röhm, 2013).

Säkerheten av den personliga integriteten är ett otroligt dagsfärskt ämne, inte minst utifrån vad som hände i den stora skandalen kring Facebook och Cambridge Analytica (Aziza, 2018). Söker vi efter begreppet på exempelvis Google eller Google Scholar, kan vi se hur personlig integritet är ett utforskat ämne. Däremot har vi fått en uppfattning om att begreppet har en evinnerlig relevans och behov av vidareforskning, då begreppet används frekvent av oss i vardagen. Trots begreppets ständiga närvaro, verkar det dock inte ha någon globalt överenskommen och fastslagen definition. Detta är något som inte heller det svenska utrikesdepartementet kunnat fastslå, där de förklarar hur *"Någon allmängiltig definition av begreppet har dock inte slagits fast i lagstiftningen"* (SOU 2017:52) .

I en studie skriver Balebako et al. (2013) hur 68% av dess undersökta smartphones-användare inte var medvetna om att dess data delades i marknadsföringssyfte. I studien beskrivs hur en av de deltagande berättat hur denne upplevde omedveten spridning av data som ytterst upprörande, eftersom hen ville vara så anonym som möjligt. Vidare förklarar författarna hur de kunnat konstatera att studiens deltaganden har missuppfattningar kring den delning av data som sker via smartphone-applikationer och att majoriteten bryr sig om ifall program delar sekretesskänslig information med tredje part eller inte.

Quah & Röhm (2013) skriver även i en studie hur många användare av molntjänster, inte har läst sekretessvilkoren innan de använder tjänsten. Trots detta, förklarar de hur majoriteten av användarna är medvetna om vissa förekommande och gränsöverskridande dataflödesfrågor, men att de fortsätter använda sig av tjänsterna på grund av att tjänsternas fördelarna och bekvämlighet överväger riskerna.

I en annan studie belyser Struse et al. (n.d.) potentiella säkerhetsrisker som kan uppstå om användare är oförmögna att förstå användarvillkoren. Dessa studier tydliggör för de problem och risker som kan uppstå ifall användare inte besitter tillräckligt med kunskap om hur data samlas in

och delas av smarta enheter och molntjänster. För att försöka ta reda på hur dessa problem och risker kan undvikas samt hur företagen bör gå tillväga för att öka användarnas medvetenhet kring vilken data som samlas in och används, valde vi att undersöka området ur användarnas perspektiv.

1.3 Problemformulering

Enligt Jacobsson et al. (2015) beräknas runt 90 miljoner människor bo i smarta hem inom en snar framtid. Det smarta hemmet är ett fenomen som utgår från tekniken Internet of Things och används för att förbättra såväl bekvämlighet som säkerhet för användarna (Jacobsson et al. 2015). Enligt Bugeja, Jacobsson & Davidsson (2016) visade en studie på hur marknaden för smarta enheter värderades till 9,8 miljarder USD år 2015 och estimerades att uppnå ett värde på 43 miljarder år 2020. Enligt en ny studie från samma källa kan vi bekräfta en realisering av estimatet, vilken påvisar att intäkterna för marknaden av smarta enheter år 2018 uppgår till ett värde av lite drygt 46 miljarder USD (Statista, 2018b). Studien visar även statistik på hur marknaden förväntas ha en årlig tillväxt på 25% under de nästkommande åren, och uppskattar ett marknadsvärde på nästan 113 miljarder USD år 2022.

Med detta som grund, kan vi alltså konstatera att marknaden för smarta hem har och fortsätter genomgå en rejäl tillväxt. Men med denna marknadstillväxt ökar även antalet internetuppkopplade enheter i hemmet, vilket exponerar hushållens medlemmar för ännu fler integritets- och säkerhetsrelaterade risker (Bugeja, Jacobsson & Davidsson, 2016). Och med fler uppkopplade enheter ökar även datainsamling, vilket potentiellt kan bidra till stora flöden av digitalt lagrad information som kan klassificeras som big data (SAS, n.d.). Det ena skälet till den rejäla tillväxten för IoT-produkter är att det har blivit mindre kostsamt att koppla upp olika enheter till wifi och på så vis blivit mer populär att använda (Morgan, 2014).

Vidare antyder Bugeja, Jacobsson & Davidsson (2016) att de ökade riskerna är en konsekvens av att data blir åtkomstbar genom de nätverk som de är uppkopplade mot, vilket resulterar i att privat och känslig information blir enklare att komma åt och hanteras via fjärrstyrning. Om en obehörig part lyckas ta sig in på nätverket, som följd av säkerhetsbrister i enheternas och systems datahantering, kan angriparna få tillgång till ytterst känslig data. Används tekniken i molnet, som levererar olika tjänster, möjliggörs även tillgång till data från olika enheter och kontext (Mell & Grance, 2011). Det smarta hemmets användare riskerar därmed att utsättas för integritetskränkning, och diverse komplikationer. Till exempel kan användarna utsättas för identitetsstöld eller i värsta fall för livshotande skador, om exempelvis medicinsk- och hälsorelaterad data görs icke-åtkomstbar för användaren eller manipuleras av den obehöriga parten utan hushållets vetskap.

Enligt Bugeja, Jacobsson & Davidsson (2016) är integritetsrelaterade problem otroligt invecklade och inte alltid särskilt uppenbara och lättolkade. Det är därför viktigt att användarna är medvetna om hur tekniken ska användas för bekvämlighet och komfort samtidigt som den inte äventyrar säkerheten för insamlad data och deras personliga integritet. Tillverkarna av de smarta enheterna behöver tydliggöra vad för data som samlas in samt hur den hanteras och lagras, vilket skulle underlätta för det smarta hemmets användare att hitta och förstå information om vad för data som berörs.

1.4 Forskningsfråga

Ur ett användarperspektiv - Vad indikerar pålitlighet inom ett smart hem där data delas per automatik via smarta enheter?

1.5 Syfte

Med vår studie vill vi, genom att utföra intervjuer och samla in teoretiskt material, komma fram till en slutsats för vad som indikerar pålitligheten för de smarta hemmets användare vid användning av enheterna.

1.6 Avgränsningar

Studien beaktar hur det smarta hemmets användare uppfattar de smarta enheternas pålitlighet i förhållande till insamling och hantering av data. Vi undersöker även en leverantör av det smarta hemmets enheter samt en av de svenska säkerhetsmyndigheternas ställningstagande till hur företag samlar in och hanterar data samt vilken roll användarna har i det hela. Detta görs för att få en bättre förståelse för vilka aspekter som är viktiga att ta i beaktning för företag vid insamling och hantering av personlig data. Studien fokuserar på den svenska marknaden, vilket är anledningen till varför vi endast valt att intervjua användare som bor i Sverige, en leverantörer som är baserad i Sverige samt en svensk säkerhetsmyndighet.

Uppsatsen berör tekniska områden ytligt. Vi beaktar därför inte djupgående tekniska aspekter som förekommer vid insamling och hantering av data. Detta eftersom uppsatsens fokus ligger på användarens synvinkel på den personliga integriteten samt pålitligheten vid användning utav smarta hemmets enheter och inte den tekniska processen. Eftersom uppsatsen även riktar sig mot användare med blandad teknisk bakgrund och kompetens samt åldrar, har vi försökt att endast använda simpla och pedagogiska beskrivningar av begreppen.

2. Litteraturgenomgång

I vår litteraturgenomgång introduceras läsaren för den teori som använts genom studiens gång. Detta kapitel börjar med att presentera de tekniska aspekterna av studien, följt av områden som berör det smarta hemmets användare med fokus på den personliga integriteten. Vidare presenteras det ramverk och den modell som studien använder sig av. Slutligen knyts litteraturgenomgångens kapitel ihop med en sammanfattning, där samtliga berörda ämnen konkluderas.

2.1 Teori

2.1.1 Motivering för val av teori

Smarta hem
Teorin för det smarta hemmet har valts ut för att ge användaren en förståelse till fenomenets evolution, snabba utveckling och funktionalitet. Vi har valt att presentera en elementär bild av det smarta hemmet genom den uppdelning Bugeja, Jacobsson & Davidsson (2016) gör av det smarta hemmets beståndsdelar. Uppdelningen reducerar den komplexa arkitekturen av det smarta hemmets och erbjuder läsaren en simpel och överskådlig bild för hur det smarta hemmet fungerar och hur dess olika delar samarbetar.

Internet of Things (IoT)
Studien behandlar IoT eftersom det är den tekniken som de smarta enheterna utgörs av. Botta et al. (2015) beskriver hur IoT ofta karaktäriseras av *"[...]real world small things, widely distributed, with limited storage and processing capacity, which involve concerns regarding reliability, performance, security, and privacy."*. En definition som tydliggör begreppets relevans för vår studie.

Modellen för IoT's generiska arkitektur hjälper oss att förstå den grundläggande tekniken bakom de smarta enheternas processflöde, för hur data samlas in till att ett värde genereras. Vidare hjälper modellen oss att se vart den personliga integriteten påverkas som mest vid de smarta enheternas datahantering, samt var den personliga integriteten kan tänkas vara mest sårbar i datahanteringsprocessen.

Molntjänster
Molntjänster är en annan teknik som ofta används inom det smarta hemmet. Mell & Grance (2011) definition av begreppet - *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources*

(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" - tydliggör varför tekniken är tillämpbar för vår studie. Genom att undersöka begreppet, hjälper vi till att öka läsarens förståelse för tekniken bakom den överföring och hantering som sker av data som samlas in genom de smarta hemmets enheter.

Big Data
Eftersom statistik visar hur marknaden för smarta hem ständigt växer (Statista, 2018b), ger denna teoridel substans för att kunna visa hur det smarta hemmet bidrar till ökad datainsamling ur ett globalt perspektiv.

Data Analytics
Ämnet undersöks för att förstå hur rådata kan extraheras till värdefull information och i slutändan påverka den personliga integriteten. Med hjälp av denna teoridel vill få en bättre förståelse för vilka konsekvenser som kan uppstå genom att olika typer av insamlad persondata kombineras och analyseras.

Big Data's Dimensioner
Ramverket för big data tydliggör hur värdefull information kan genereras från rådata. Samtidigt visar ramverket för risken samt möjligheterna med analys av rådata. Genom att sätta det smarta hemmet i perspektiv till dessa dimensioner, hoppas vi kunna förstå hur de smarta enheternas insamlade data potentiellt kan påverka dess användare.

CIA-Modellen
Modellen vägleder vid utformandet av policyer, där fokus ligger på informationssäkerhet. Genom att undersöka modellen, ger det oss en bättre förståelse och inblick i hur information klassificeras samt bör hanteras i förhållande till faktorerna tillgänglighet, integritet och konfidentialitet. Detta är viktigt för oss att förstå, för att kunna undersöka hur data kan påverka den personliga integriteten.

2.1.2 Smarta Hem

Historia
Under flera decennier var idén om smarta hem något som existerade i enbart science-fiction-världen (Hendricks, 2014). Under tidigt 1900-tal introducerades maskiner i hushåll, där det år 1901 lades ett patent på en motordriven dammsugare som monterades på en hästvagn, av den brittiske civilingenjören H.Cecil Booth (National Academy of Engineering, 2018). Denna uppfinning var ett av startskotten till vad som skulle komma att uppfinnas, med mål om att underlätta de vardagliga hushållsuppgifterna med hjälp av tekniska lösningar.

Under 1960-talet började dock mänskligheten laborera med samt lansera produkter inom ramen för dagens benämning av "smarta hem" (Hendricks, 2014). Men det var däremot inte förrän tidigt 2000-tal som populariteten av smarta hem började växa sig allt större och fler hushåll såg ett verkligt värde av dess användningsområde. Hendricks (2014) beskriver hur denna era började erbjuda teknik och enheter för smarta hem som var prisvärda även för den vardagliga individen, vilket ledde till att dessa syntes allt mer på marknaden och i hemmen.

År 2014 blev ett stort genombrott för dagens marknad av smarta hem, då tre av dagens mest välkända företag - Apple (2014), Samsung (2014) och Amazon (2017) - lanserade sina första upplagor av enheter för smarta hem. Idag finns det dock ett flertal tillverkare och nyckelspelare som har brottat sig in på marknaden för smarta hem, där efterfrågan och intresset för hemautomation fortsätter öka bland såväl privatpersoner som företag (MarketsandMarkets, 2017). Däremot har även det kritiska ögat stärkts, för huruvida säkert, etiskt korrekt och vinstgivande det är för användarna i förhållande till den guldgruva av data som användarna "betalar" med till företagen. Norton (2018) skriver om en del av de säkerhetsrelaterade risker som smarta hem medför, där insamlandet av data och risken för dataintrång nämns. Trots riskerna, tyder dock statistik för de smarta hemmens marknadstillväxt (Statista, 2018b) på att detta inte verkar vara ett tillräckligt stort problem för att hämma marknadens tillväxt - än.

Vad är Smarta Hem?

Ett samlingsbegrepp för tekniker som, genom en central styrning, automatiserar och förenklar hanteringen av elektroniska enheter i hemmet. Genom fjärrstyrning är samtliga enheter som kopplats till den centrala åtkomstpunkten övervaknings- och kontrollerbara överallt i världen genom mobilen eller annan nätverksenhet (Investopedia, 2018b).

Bugeja, Jacobsson & Davidsson (2016) beskriver hur ett smart hem, i grund och botten, är en kombination av *enheter*, *kommunikation* och *service*.

Enheterna

Utgörs av hårdvaruenheter som karaktäriseras av sensorer, portar, ställdon och 'smarta föremål'.

Kommunikation

Syftar på den stora variation av kommunikationsprotokoll som smarta hem använder sig av och kopplar upp sig mot. Dessa innefattar allt från kabel- till radiobaserade kommunikationsprotokoll. Det är här enheterna "pratar" med varandra.

Services

Denna term inbegriper de mjukvaruapplikationer som hanteras i molntjänster eller innanför den hemmiljö som bland annat ansvarar för implementationen av automatisering, enhetshantering

och beslutsfattande. För att interagera med och kontrollera uppkopplade enheter i det smarta hemmet, sköts interaktionen vanligtvis genom särskilda kontroller vars mjukvara ofta körs via smartphones eller tablets. Dessa kontroller gör det möjligt att interagera med enheterna, såväl lokalt som genom fjärrstyrning.

Sammanfattningsvis kan vi se hur det är *enheterna* som samlar in data, *kommunikationen* som överför data och *services* som levererar värdet och funktionerna.

Det smarta hemmets hanterings- och applikationsområden

I sin artikel "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources,", definierar Mendes et al. (2015) det smarta hemmet som en hemmaliknande miljö som har omgivande intelligens och automatiserad kontroll samt besitter förmågan att reagera på invånarnas beteende och erbjuda anpassade lösningar. Vidare nämner de hur det smarta hemmets enheter brukar kategoriseras in i fyra olika områden - underhållning, energi, säkerhet och hälsa - eftersom de ofta hanterar olika data och appliceras inom olika områden i bostaden.

Det smarta hemmet i förhållande till det traditionella

Så vad är det som främst skiljer ett smart hem ifrån ett traditionellt? Svaret är relativt simpelt. I det traditionella hemmet kontrolleras och sköts vardagliga sysslor manuellt, där utförande av uppgifter kräver en mänsklig interaktion. I det smarta hemmet däremot, kan majoriteten av de vardagliga sysslorna skötas och kontrolleras genom trådlösa nätverk och automatiserade system (Mendes et al. 2015). Exempelvis, om du inte ska sluta upp med ett tomt kylskåp krävs det att du går och tittar i kylskåpet för att veta vad som behövs. Sedan behöver du antingen komma ihåg vad som behövs handlas in eller skriva ner det för att inte glömma handla alla varor. Därefter behöver du antingen gå in och beställa hem maten online eller åka iväg och handla den mat som behövs i en fysisk butik. I ett smart hem däremot, är kylen förmodligen utrustad med sensorer och teknik där, bland annat, kylskåpet kan visa direkt i mobilen vilka matvaror du har kvar och vad som behövs handlas in. Vilket låter dig göra detta från bland annat matbutiken. Dessutom kan du som användare, skapa din egna kalender på touchskärmen som finns på kylskåpet, eller kolla upp nya recept. Allt detta görs via hub, som sparar och kommunicerar med applikationerna som finns till kylskåpet (Samsung, n.d.).

Det tänkta värdet med det smarta hemmet i förhållande till det traditionella, är att samtliga enheter, enskilt och tillsammans, ska utföra vardagliga uppgifter i hemmet för att underlätta vardagen samt för att spara pengar, tid och energi åt användaren (Kovach, 2015).

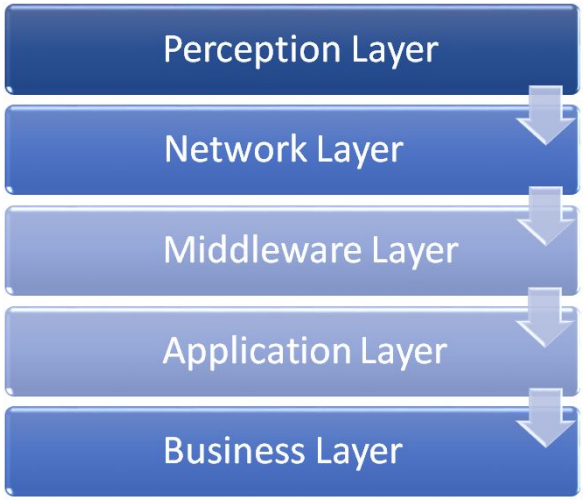
2.1.3 Internet of Things (IoT)

Smarta Hem-system är baserade på Internet of Things (IoT), en teknik som för första gången föreslogs år 1999 av den brittiska och teknologiska pionjären Kevin Ashton (Ashton, 2009). Idag har tekniken som skapar möjligheten för att koppla upp olika enheter till wifi blivit allt mindre kostsam och allt mer populärt att använda, både ur ett tillverkar- och användarperspektiv (Morgan, 2014). IoT avser ett nätverk, vilket består av fysiska objekt som kan samla in och dela elektronisk data och information. Begreppet utgörs av en mängd olika smarta enheter, som kan vara alltifrån stora industriella maskiner som utför dataöverföring mellan varandra till sensorer som samlar in data om människokroppen (Investopedia, 2017). Investopedia (2017) beskriver hur det huvudsakliga syftet med IoT är att skapa enheter som, genom sig själva och per automatik, ständigt uppdateras i realtid samt förbättrar effektiviteten och identifierar viktig information snabbare än system som är direkt beroende av mänsklig interaktion.

Arkitekturen av IoT

Det finns ingen enskild konsensus för arkitekturen av IoT, som godkänts genom en universell och gemensam överenskommelse. Istället finns ett flertal modeller för huruvida dess arkitektur bör definieras och visualiseras, vilka framtagits genom olika studier och forskare. Efter att ha tittat på ett flertal studier har vi, likt Sethi & Sarangi (2017), kunnat konstatera att det främst är två arkitekturer som är ständigt förekommande vid studier av IoT: en tre- och femlagersarkitektur.

Den mest grundläggande är trelagersarkitekturen, som introducerades i tidigt stadie av forskningen kring IoT (Sethi & Sarangi, 2017). Denna arkitektur utgörs av tre skikt: Perception Layer, Network Layer & Application Layer. Arkitektur hjälper till att definiera huvudsyftet med IoT, men är oftast inte tillräcklig i forskningssammanhang av ämnet eftersom den inte klarar av att hantera de mer detaljerade aspekterna som då krävs. På grund av detta har en femlagersarkitektur utvecklats, där ytterligare två lager har applicerats: Middleware Layer och Business Layer (Khan et al. 2012).



Figur 1 - IoT's Generiska Arkitektur

Perception Layer
Detta lager innefattar det fysiska lagret, vilket utgörs av fysiska objekt och sensorer som letar och samlar in data om miljön de befinner sig i. I korta drag är det i detta lager som identifiering och insamling av objektspecifik information sker genom de olika sensorenheterna (Farooq et al. 2015). Beroende på vilken typ av sensor som används, kan den insamlade datan innefatta allt från temperaturer till platsspecifika koordinater. När insamling av data utförts, skickas den data sedan vidare till *Network Layer* (Khan et al. 2012).

Network Layer
Hit kommer all insamlad data som tillhandahållits i Perception Layer, för att på ett säkert sätt kunna överföras från de sensorstyrda enheterna till informationshanteringssystemen. Överföringen kan ske genom ett flertal olika kommunikationsnätverk, där Wifi och bluetooth är två av många exempel (Khan et al. 2012). Lagret ansvarar bland annat för uppkopplingen till andra smarta enheter, nätverksenheter och servrar (Sethi & Sarangi, 2017). Således kan vi alltså konstatera att detta lagret av IoT, sköter dataöverföringen mellan *Perception Layer* till *Middleware Layer*.

Middleware Layer
Detta lager utgörs av informationshanteringssystem som hanterar och analyserar den insamlade datan som överförts via *Network Layer*. Khan et al. (2012) beskriver hur det, utöver informationshanteringen, även är i detta lager som ubikvitära beräkningar av den insamlade datan sker. Baserade på de resultat som datahanteringen genererat, utför sedan systemen automatiserade handlingar och tar automatiserade beslut samt länkar samman systemen till den databas som tillhandahåller lagringsmöjligheter för den insamlade datan (Farooq et al. 2015).

Vidare beskriver de hur detta lager är serviceorienterat och därmed garanterar samma servicetyp mellan de anslutna enheterna.

Application Layer
Det är i detta lager som en mängd praktiska tillämpningar av IoT, som är baserade på användarnas behov, realiseras. Utöver användarnas behov, kan dessa praktiska tillämpningar även baseras på olika branschers behov, där bland annat smarta hem är ett exempel på en applikation som implementerats genom IoT (Farooq et al. 2015). Det är även detta lager som realiserar fullständig hantering och administrering av de praktiska tillämpningarna, utifrån den objektspecifika information som hanterats i *Middleware Layer* (Khan et al. 2012).

Business Layer
Khan et al. (2012) beskriver hur detta lager ansvarar för hanteringen av samtliga IoT-system, inklusive applikationer och tjänster. Det är här som processkartor, grafer och statistik skapas och utvecklas, baserat på den data som tagits emot från *Application Layer*. Vidare förklarar de hur lagret, till stor del, handlar om att omvandla data från *Application Layer* till något av värde och därmed något vinstdrivande. Exempelvis: kunddata omvandlas till strukturerad information som genererar ett värde i form av utökad kunskap om efterfrågan. I slutändan resulterar det i att tillverkaren tjänar mer pengar på sin tjänst, som en följd av förändrade strategiska beslut som kunnats ta utifrån den kunskap som erhållits kring exempelvis marknadsförändringar.

2.1.4 Cloud Computing - Molntjänster

Idag används molntjänster oftare än vad användaren kanske är medveten om, där användningen av online tjänster för email (Microsoft Azure n.d.a) är ett exempel. Förenklat beskriver Microsoft Azure (n.d.a) hur molntjänster är den leverans som sker av datatjänster över internet (the cloud/molnet). Dessa datatjänster inkluderar bland annat databaser, lagringsutrymmen och mjukvara. Molntjänster möjliggör dessutom för att exempelvis funktionerna för ett styrsystem kontrolleras via en mobiltelefon och därmed är tillgängliga över ett nätverk (Mell & Grance, 2011). Exempel på funktioner för en användare kan vara att redigera dokument, spara och kolla på bilder samt lyssna på musik.

Microsoft Azure (n.d.b) beskriver molnet som en pool av datorresurser som är uppkopplad via internet. Vidare förklarar de hur molnet fungerar likt ett globalt nätverk som fungerar likt ett ekosystem som består av servers, där varje server har en unik funktion. Dessa servrar lagrar och hanterar data, samt kör olika applikationer eller program för att leverera olika tjänster, vilket sker per automatik efter behov och kräver därför ingen mänsklig interaktion med tjänstleverantörerna (Mell & Grance, 2011).

Istället för att exempelvis lagra filer i en lokal enhet, möjliggör molntjänster användning av fjärrdatabaser (Investopedia, 2018a).

2.1.5 Big Data

När det idag talas om 'Big Data' syftar den relativa termen oftast till stora volymer av såväl ostrukturerad, semistrukturerad som strukturerad data och som har potential att brytas ned eller formas till information (Bigelow & Rouse, 2016). Vidare beskriver termen även den situation då mängden data överstiger volymen för de traditionella programmens och systemens lagrings- och beräkningskapacitet (ComputerSweden, 2018), och därmed vad som är hanterbart i förhållande till särskiljande, analys och lämpligt beslutsfattande av datan (Perwej, 2017).

Oavsett huruvida big data är strukturerad, tydliggör ett flertal studier att termen alltid har förmågan att generera något form av värde i slutändan. Perwej (2017) beskriver hur hanteringen och integreringen av en mängd olika data och information, ofta flera varandra oberoende komponenter, är vad som i slutändan genererar värdet. Han nämner även att den största anledningen till skapat värde ligger i vad parten väljer att göra med de insamlade uppgifterna. Analysen av datan är därmed den mest kritiska och betydande delen i vilket värde och information som genereras i slutändan.

2.1.6 Data analytics

För inte allt så länge sedan insåg organisationer att data som flödar inom företaget, mycket möjligt kan vara mer värdefullt än guld. Anledningen till detta är att det går att använda sig utav samma data för olika motiv (Informatica, n.d.).

Syftet med att använda sig utav data analytics är att extrahera meningen från rådata med hjälp av system. Detta utförs genom användandet av algoritmer som identifierar mönster i data, vilket kan ger insikt i huruvida beslut ska tas och hanteras (Leuschner, 2017). Mer detaljerat transformerar, planerar och gör de modeller av data, för att sedan kunna hitta mönster och dra slutsatser (Informatica, n.d.). Data analytics hjälper, exempelvis, organisationer att bättre förstå sin verksamhet och hur de ska förbättra den.

Data analytics är en aspekt som förväntas främja det smarta hemmet i framtiden. Detta eftersom data analytics hjälper till att ge de smarta enheterna, som är integrerade genom IoT, ökad medvetenhet för fler och större delar av hushållets olika delar och funktioner (Leuschner, 2017). Exempelvis kan det röra sig om alltifrån smarta termostater till smarta kylskåp. Eastwood (2017) nämner bland annat hur en av de största fördelarna med att använda data analytics i det smarta hemmet, är dess förmåga att skapa smarta och integrerade system som reagerar i realtid utefter användarens behov.

Trots de många fördelarna som uppkommit genom interaktionen av data analytics med det smarta hemmet, nämner Leuschner (2017) att det fortfarande finns en hel del säkerhetsrelaterade utmaningar att tackla innan det är ett fullbordat koncept. Han nämner bland annat hur integritet och säkerhet av data är två kritiska faktorer som behöver beaktas innan det smarta hemmet kan anses som säkert. Vidare belyser han dessutom vikten av att se problemet ur en realistisk synvinkel, för att kunna hitta reella lösningar.

2.1.7 Personlig integritet

Idag är möjligheterna stora att snabbt kunna sprida information i omvärlden, där bland annat personlig information och information om händelser delas via internet (Dir 2014:65). Det är inte endast individens intresse att använda sig utav dessa medel på internet, utan även företag har sett stora och nya möjligheter att bedriva sin verksamhet genom dessa lättillgängliga metoder. På så vis kan företag effektivisera sina processer och även nå en större kundkrets (Dir 2014:65). Vidare skriver justitiedepartementet i kommittédirektivet (Dir 2014:65) hur informationen gör det även möjligt för företagen att kunna kartlägga den enskildes beteendemönster på internet, vilket leder till att företagen bättre kan förstå sina kunders behov och agerande samt hitta nya möjligheter till affärer.

Det som skrivs i kommittédirektivet från justitiedepartementets (Dir 2014:65) är att dagens teknologi bland annat har gjort det enklare för företag att utnyttja nya möjligheter som uppstår genom tekniker som datalagring och analysfunktioner, däribland molntjänster. Vidare nämner de att även om teknologin kommer med en hel del möjligheter, sätter den också press på företagen eftersom den medför nya risker och utmaningar för intrång i den personliga integriteten. Dessa risker är något som företagen måste förhålla sig till genom att följa PuL.

Som tidigare nämnt, finns ingen globalt överenskommen och fastslagen definition av begreppet personliga integriteten. Trots att det svenska utrikesdepartementet, valt att utelämna någon allmängiltig definition av begreppet i en av deras lagstiftningar (SOU 2017:52), förklarar dock justitiedepartementet i ett av sina kommitédirektiv hur de valt att använda begreppet för att beteckna den enskildes värde och värdighet (Dir 2014:65). I kommittédirektivet från justitiedepartementet (Dir 2014:65) förklaras även hur personlig integritet går hand i hand med den enskildes privata information och rätten att få kontrollera vem som ska ha tillgång till denna information. Personuppgiftslagen (PuL) har som syfte att genom lag att skydda den enskildes personliga integritet. Lagen ser till så att den personliga integriteten inte kränks genom behandling av personuppgifter, där all information som är kopplat till en fysisk person ska skyddas (Personuppgiftslagen SFS 1998:204). Den 25:e Maj kommer dock lagen att upphävas och istället ersättas av Dataskyddsförordningen (GDPR), vilken innebär ytterligare stärkt skydd av känsliga personuppgifter (Datainspektionen, 2017a).

Kommittédirektivet ser ett behov av att genomföra en kartläggning och analys av de risker som uppkommer för intrång i den personliga integriteten. De anser att detta behov blir större på grund av den tekniska utvecklingen där användningen av informationsteknik i verksamheter är allt vanligare (Dir 2014:65).

Molntjänster och integritet

Då smarta hemmets enheter är oftast uppkopplade till molntjänster för att kunna kommunicera, dela data med varandra, uppstår några juridiska frågor när den personliga integriteten kommer på tal (Agarwal & Agarwal, 2011). Dessa frågor berör olika risker med vad som kan hända med den personliga integriteten när data delas via olika kanaler. Vidare förklarar Agarwal & Agarwal (2011) hur ytterligare risker som är värt att beakta, är huruvida användare oavsiktligen ger bort sin personliga information genom att publicera data i Cloud. Då personlig information ges bort, uppstår risken för att den datan används för andra ändamål än det egentliga syftet, som inkluderar annonsering.

Individens rättigheter

En individ bör veta och se vilken data som samlas in om dem och de bör också ha möjligheten till att styra vilken data som ska samlas in och hur mycket samt vad som ska raderas. Rättigheten till att en individ ska kunna ha tillgång till samt utmana sin egna datainsamling är en utav de viktigaste säkerhetshandlingarna för att skydda sekretessen, vilket då tillåter datainsamlingen att vara transparent (Anandarajan & Simmers, 2018). Individers möjlighet att vara medveten om att behandling av hens personuppgifter sker, är bland annat en aspekt som GDPR kommer försöka stärka när den träder i kraft den 25:e maj (Datainspektionen, 2017b). Datainspektionen (2017b) skriver hur de arbetar för att stärka individers rättigheter när det kommer till skyddandet av den personliga integriteten.

Inbyggd integritet

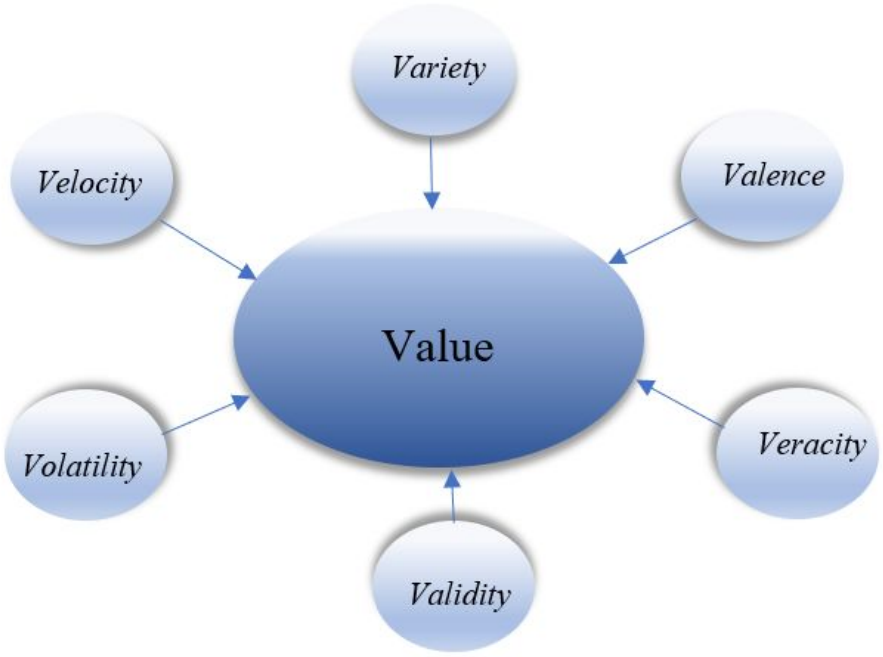
Inbyggd integritet eller privacy by design används vid utveckling av system för att skydda den personliga integriteten. Datainspektionen (2012) förklarar vikten av att beakta integritetsaspekterna, i ett tidigt skede av utvecklingen av system, för att undvika att behöva rätta till misstagen som vid senare skede i processen kan bli dyra att fixa till. Vilket är därför viktigt att låta integritetsfrågorna påverka hela systemet livscykel. En viktig integritetsaspekt är bland annat att skydda personuppgifter (Datainspektionen, 2012).

Datasekretess

Datasekretess finns i den utsträckning som organisationer eller individerna tillåter den att vara i, vilket menas med att organisationer och individer bestämmer själva vilken data i ett system som ska delas med en tredje part. När personlig information samlas in, lagras eller används, berörs integriteten och blir därför ett integritetsproblem. Frågan som uppstår därför är vem som äger datan, vilket kan därför vara en rättslig fråga (Robinson, 2018).

2.2 Ramverk och Modeller

2.2.1 Big Data's Dimensioner



Figur 2 - Sambandet mellan big data's dimensioner.

För att tydliggöra begreppet 'Big Data' samt hur och varför det är en kritisk faktor vid framtagandet av värdefull information, konkretiserar vi dess egenskaper genom ett ramverk som delar upp benämningen i sex komponenter - Volume, Velocity, Variety, Veracity, Valence, Volatility. Med denna konceptuella generalisering, förtydligar vi hur dessa byggstenar tillsammans expanderar datans struktur till något användbart: Value.

Volume, Velocity, Variety och Veriacity är fyra dimensioner som ofta brukar användas i samband med definitionen av big data (Perwej, 2017) och dess värde. I vår studie adderar vi även Volatility och Validity för att förklara ännu fler dimensioner av big data, eftersom de bidrar med ett värde i analyseringsprocessen för smarta hems hantering av data. Detta eftersom det kommer förtydliga vidareanalyser av exempelvis kopplingen mellan olika typer av data samt klassificering av real-time-data's trovärdighet och giltighet.

Volume - Storleken av data
Volymen syftar på mängden data som alstras varje sekund och refererar till storleken av den data som samlas in och skapas från alla olika källor, oavsett om det innebär ett foto, medicinsk data,

en kommunikationstråd från sociala medier eller väderleksrapporter (Dumbill, 2012). Just i denna sekund genereras mer och nya mängder data via nätverk, maskiner och mänsklig interaktion med system som sociala medier. Exempelvis, tänk efter hur många twitter-meddelanden och instagram-inlägg som publiceras varenda dag. Volymen av data växer hela tiden och snabbt, vilket försvårar hanteringen av den.

Som en följd av den enorma mängden data som existerar och samlas in, försvåras hanteringen av den för olika informationshanteringssystem. Big Data system kan, pga volymen, inte längre hanteras eller behandlas genom traditionella metoder som SQL. Ali-ud-din Khan, Uddin & Gupta (2014) exemplifierar detta genom att förklara hur det inte längre går att skriva en query likt *"select something from some table where something equals something"*, eftersom ostrukturerad data inte är i närheten av att kunna normaliseras på det sätt vi är vana vid när det gäller hantering av tables och data sets.

Velocity - Hastigheten för att analysera dataströmmar
'The Velocity' refererar till den hastighet som ny data uppstår, men även hastigheten det tar för datan att reinkarneras och alstras (Perwej, 2017). Termen redogör hastighetens betydelse för hela processen av datainsamling till beslutsfattande. Viktigt att förstå är att termen inte enbart avser den stora mängden och hela tiden inkommande datan, utan även betydelsen av det som Dumbill (2012) förklarar som en återkopplings-loop. Det vill säga, att ta data från input och transformera det till ett beslut. Han trycker mycket på hur hastigheten till data output också är en otroligt viktig faktor i förhållande till processen för värdeskapandet av data.

> *"The tighter the feedback loop, the greater the competetive advantage."* (Dumbill, 2012).

Hastigheten är en av de aspekter som direkt kan utpekas till "skuldbärare" för den stora volymen av data som ständigt alstras. Det är hastigheten av data som gör att data inte längre blir hanterbar. Laney (2001) beskriver hur det ställs nya krav på utformandet av datahanteringssystem där de behöver ha otroligt dynamiska och disponibla lösningar för behandling av samt lagringskapacitet för data. Något som beskrivs likt en konsekvens av den höga hastigheten och därmed mängd som ny data ständigt genereras, exempelvis genom användandet av internet och sociala medier.

Variety - Olika former av data
Det är väldigt sällan som information presenterar sig själv perfekt organiserat, fullt förståeligt och specifikt kopplat till rätt sammanhang och resultat. Ofta gäller detta även i sammanhang med big data, där en gemensam nämnare är mångfaldig och diverse data som till varandra är oberoende komponenter. Big data finns i alla olika former, och när det talas om variation i förhållande till big data innebär det därför allt ifrån innehåll, kontext och datatyp (Dumbill, 2012). På grund av dess alla olika former, genereras en otrolig komplexitet gällande dess

hantering och det går därför inte att hantera den genom vad vi tidigare känner igen som relationsdatabaser (Ali-ud-din Khan, Uddin & Gupta, 2014).

Ett vanligt användningsområde vid hantering av big data, är att utvinna efterfrågad och korrekt mening av ostrukturerad data. Det handlar bland annat om processen för att bestämma exakt vad ett namn ska avse. Exempelvis, när användaren av ett system söker på staden Sydney, ska systemet då söka efter och visa information om Sydney i Australien eller Sydney i Kanada? För att rätt resultat ska genereras, behöver alltså en klassificering av entiteter ske. Samtidigt som en stor variation av data kan vara gynnsamt för att skapa en bred, djupgående och rättfärdig analys, konkretiserar dock Perwej (2017) hur detta skapar en utmaning för exempelvis företag och deras datasystem vid insamling, sortering och lagring av all data. Stor variation av data och information betyder även större utmaning att hitta och generera rätt kaliber.

Valence - Samhörigheten av big data
Valence mäter sambandet mellan den data som samlas in och undersöker sedan om det eventuellt finns en direkt eller indirekt koppling mellan de olika komponenterna (Atanassov et al. 2016). En direkt koppling kan exempelvis vara att två instagram-användare följer varandra, medan en indirekt koppling kan vara att två studenter studerar samma program fast på olika universitet. Valence däremot, är ett fragment av dataenheter som mäter förhållandet mellan faktiska samband mellan dataenheter i relation till antalet möjliga kopplingar som kan uppstå inom samlingen. Datakopplingen är något som tilltar efterhand, en process Ghosh & Nath (2016) beskriver likt en konferens där vissa deltagande forskare möter andra forskare från övriga delar av världen som de tidigare inte hade någon vetskap om, och därefter får en medvetenhet om.

Veracity - Trovärdigheten och kvaliteten av big data
Veracity hjälper till att svara på frågan hur trovärdig datan verkligen är, där det handlar om förmågan att kunna granska insamlad data på ett kritiskt förhållningssätt (Ali-ud-din Khan, Uddin & Gupta, 2014). Om vi sätter detta i förhållande till alla twitter- och facebookinlägg som ständigt publiceras, blir utmaningen ganska tydlig. Det går inte att lita blint på all data och information vi hittar utan den behöver undersökas och analyseras. Med data som härstammar från denna typ av källor (i detta fall twitter eller facebook), krävs det att innehållets pålitlighet och exakthet ifrågasätts och granskas innan den tas emot som trovärdig data. Dessutom, som ett resultat av big datas många olika former, försvåras kontroller för att hantera kvalitetsbedömningen. Därför blir Veracity ytterst viktig vid hanteringen av big data i relation till analys och resultat (Perwej, 2017).

Volatility - Datans ombytlighet och "bäst-före-datum"
Med Volatility tittar vi på hur länge data är giltig och meningsfull samt hur länge den bör lagras (Perwej, 2017). Idag, med real-time-data som är mer aktuellt än någonsin, krävs förmågan att

kunna avgöra vilken data som inte längre är av relevans för aktuella och nuvarande analyser. I förhållande till big data, är det av stor vikten att kunna särskilja vilken data som är sporadisk eller regelbunden, för att i slutändan kunna frambringa pålitliga analyser och resultat (Ali-ud-din Khan, Uddin & Gupta, 2014).

Validity - Datans validitet i olika sammanhang
Ali-ud-din Khan, Uddin & Gupta (2014) liknar Validity med Veracity, men förklarar dock att det finns viktiga skillnader mellan de två dimensionerna. De förklarar hur Validity innebär huruvida korrekt och exakt data är i förhållande till det tänkta användningsområdet. Exempelvis behöver det inte förekomma någon problematik med trovärdigheten av data, men det kan däremot uppkomma validitetsproblem om den inte förstås korrekt. Vidare förklaras hur data kan vara giltig för ett specifikt användningsområde, men ogiltigt för ett annat. Perwej (2017) beskriver hur distinktiv och giltig data är nyckeln till att kunna fatta korrekta beslut.

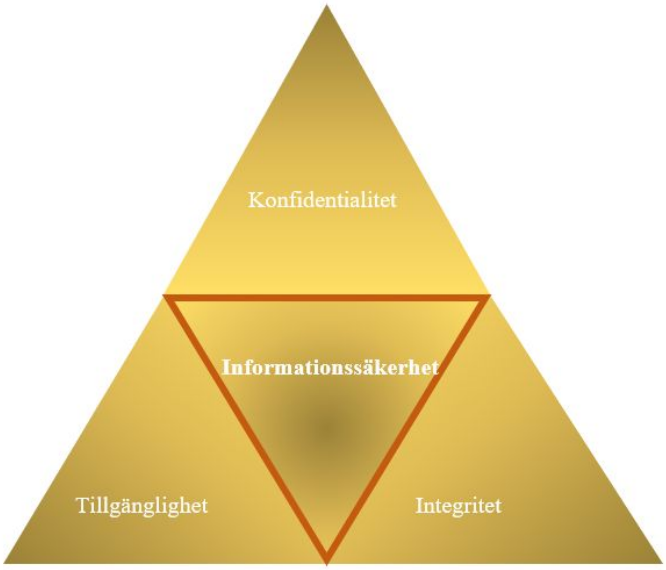
Value - Vikten av data
Detta är vad alla egenskaper av big data tillsammans arbetar mot i dess datahanteringsprocessen samt vad de i slutändan resulterar i - ett värde. 'Big Data Value' handlar om att hitta det verkliga värdet av den data vi blir tilldelade att arbeta med. Och likt det Perwej (2017) skriver krävs det att det slutliga värdet överstiger dess kostnad, ägande eller hantering av den. Värdet handlar om att göra datan identifierbar, strukturerad och därmed användbar.

Definitionen för värdet av big data har dock förändrats genom åren. Blake-Plock (2017) nämner hur big data används för att driva en mängd av automatiserade system och påpekar bland annat hur det verkliga värdet för företag inte längre handlar om hur de kan nå ut till en så bred publik som möjligt. Idag handlar det snarare om förmågan att kunna analysera och använda insamlad data för att anpassa erbjudanden så personligt och individuellt som möjligt.

"Big data can help deliver that personalized content – but not if that data is just dumped in a lake." (Blake-Plock, 2017)

Genom att förstå och undersöka alla V's av Big Data, öppnas dörrar för att hitta det verkliga värdet. Överallt gömmer sig värdefull data i mönster och information, vilken dolts på grund av mängden arbete som krävs för att extrahera den. Big data har stor potential för att generera individualiserade uppgifter och skapa verkligt värde, men för att komma dit krävs rätt verktyg samt en insikt av dess olika behov och komponenter.

2.2.2 CIA-Triad



Figur 3 - CIA-triad (Designen är inspirerad av IBM (2018) CIA "Triad").

Modellen "CIA-triad" är kärnan i informationssäkerhet där målet är att uppnå Konfidentialitet, Integritet och Tillgänglighet i informationssystemen. Med hjälp av detta ramverket strävar företag efter att kunna leverera informationssäkerhet för de enheter de säljer till sina kunder som de i sin tur använder sig utav för att kunna utföra sina uppgifter.

Konfidentialitet
Konfidentialitet i de olika system är viktigt för den enskilde individen för att uppnå målet med att hålla deras data privat och i säkerhet. Detta av den enkla anledning att data behövs för att kunna utföra tjänster samt att den blir mer värdefull vid transformationen från rådata till information. Det är därför viktigt med informationssäkerhet som kan hantera detta och det finns därför verktyg, såsom olika behörigheter i system samt krypteringar, för att uppnå konfidentialitet (Henderson, 2017). Motivet med olika behörigheter och krypteringar är att skapa begränsningar i system, så att endast behöriga personer kan få tillgång till sekretessbelagd information (Metivier, 2017).

Målet med konfidentialitet är att skapa struktur och skydda information så att den bland annat inte läcks ut. Exempel på sekretessbelagd information kan vara personuppgifter, såsom data om

deras hälsa, vilket användare vill skydda med avsikt för att inte låta obehöriga personer eller processer få tillgång till dem (Evans, Bond & Bement, 2004).

Integritet

Integritet menas med att den berättigade säkerställer att datan i ett informationssystem är pålitlig och som inte kan förstöras (Evans, Bond & Bement, 2004). Det ligger därför i användarens intresse att vara säker på att systemet följer ”code of ethics”, där användaren kan lita på att systemet uppför sig som förväntat i olika situationer (Metivier, 2017). Detta betyder också att informationssäkerheten ska vara så pass hög att det inte ska vara möjligt att en oväntad modifiering sker eller att data ska kunna bli manipulerad genom att systemet ändrar sitt beteende. Därför är det viktigt att enheterna uppnår dataintegritet, så att information endast ändras på ett speciellt eller auktoriserat sätt (Metivier, 2017). Om målet istället inte uppfylls skulle det kunna resultera i att användaren till exempel missar ett möte som har tidigare varit schemalagt, men som nu har ändrats utan användarens godkännande.

Tillgänglighet

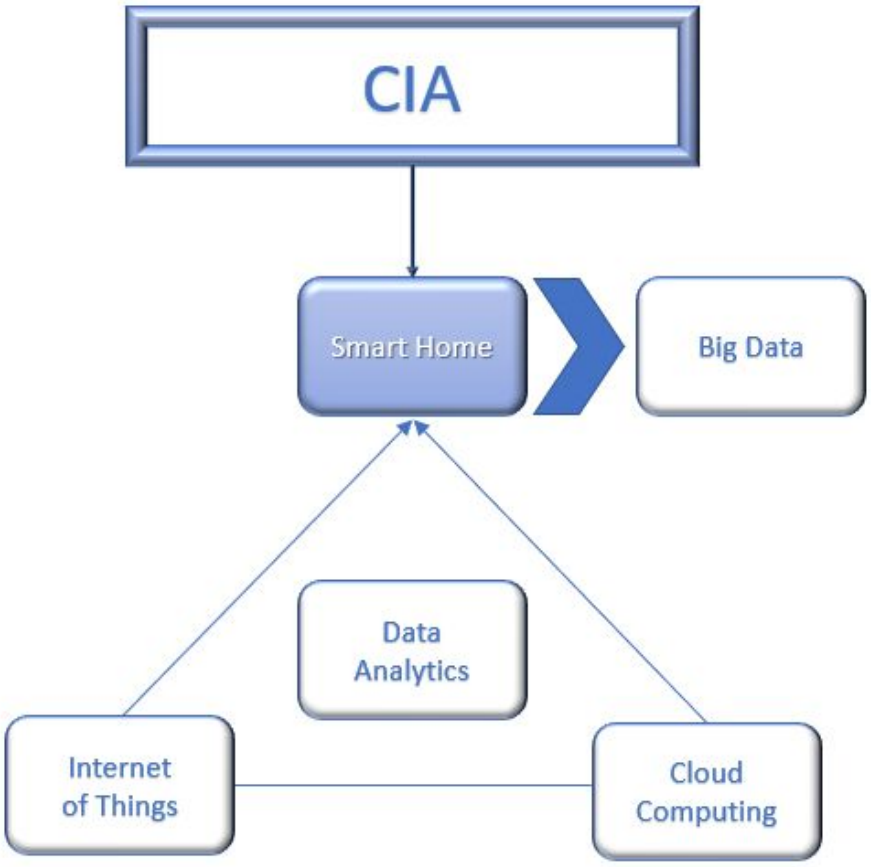
Tillgänglighet säkerställer snabb och tillförlitlig tillgång till och användning av information (Friedman & Singer, 2014). Det ska finnas garanti för en användare att användarens enheter och data ska vara tillgängliga när användaren väl behöver få tillgång till dem. Om inte, är enheterna inte tillräckligt säkra och användaren kan därför inte utföra de uppgifter som varit tänkta, till exempel att en användare inte får tillgång till sin medicinska data (Metivier, 2017), vilket skulle kunna livshotande.

2.2.2.1 Exempel på hur delar av CIA-Triad kan uppnås.

För att uppnå konfidentialitet används protokoll för nätverkssäkerhet, tjänster för datakrypteringar och nätverksautensisering i system (Agarwal & Agarwal, 2011). Dessutom kan utvecklare begränsa vart ett kortnummer bör lagras under korttransaktioner. De olika platserna där kortnumret kan lagras i kan vara exempelvis databaser, säkerhetskopior, och tryckta kvitton. Utvecklare har då begränsat åtkomsten till dessa kortnummer så att obehöriga inte kan hämta känslig eller privat information (Agarwal & Agarwal, 2011).

2.3 Sammanfattning

I vår litteraturöversikt har vi tagit upp ett flertal viktiga aspekter som har varit nödvändiga, för att ta itu med användarnas upplevda säkerhet i en smarta-hem-miljö. Vi började ta itu med dessa aspekter genom att först förstå och belysa trenderna med IoT och molntjänster (Cloud Computing), vilka tillsammans komponerar det smarta hemmets miljö. Vidare följer CIA-triaden, som en nyckelkomponent i arbetet mot att förstå den dataanalys (Data Analytics) som sker efter att all data samlats in från en smarta-hem-miljö. vilket vi även har bearbetat för att förstå hur rådata kan transformeras till information. Vi har även tagit statistik i beaktning de, som visar att smarta hemmet kommer att bli en väletablerad marknad inom en snar framtid och har därför valt att även undersöka hur datainsamlingen kommer att bidra till Big Data. För att förklara detta ytterligare beskriver figur 4 nedan förhållandet mellan ovan nämnda aspekter.



Figur 4 - Modell för sambandet mellan litteraturgenomgångens olika delar

Internet of Things (IoT)
Tekniken som möjliggör existensen av det smarta hemmets enheter.

Cloud Computing (Molntjänster)
Tekniken som möjliggör överföring av data som samlats in genom det smarta hemmets enheter. Onlinedata överförs mellan enheter och företagens servrar.

Data Analytics
Tekniken som analyserar rådata samt omvandlar och genererar det verkliga värdet av all data i form av information. Det är bland annat denna beståndsdel som möjliggör förbättring av de smarta enheternas funktioner, i form av individualiserade rekommendationer för användaren.

Smart Home (Smarta Hem)
Resultatet som uppstår genom en kombination av IoT, molntjänster och Data Analytics. De smarta enheterna (IoT) är de som samlar in data om användaren, överföringen av data (molntjänster) är det som gör att den insamlade datan kan förflyttas mellan en enhet till en annan för att sedan möjliggöra en kombination och analys (data analytics) av insamlad data. Tillsammans möjliggör de funktioner som kan användas för att underlätta användarens vardagen.

Big Data
Genom att marknaden för de smarta hemmet expanderar kraftigt, är det även tänkbart att de smarta enheternas datainsamling kommer bidra till det globala flödet av big data i framtiden. Som en konsekvens av detta, är big data och dess dimensioner en viktig aspekt att ta hänsyn till vid analys av resultat och framtagandet av studiens slutsats.

CIA
För att kunna bedöma huruvida det smarta hemmets informationshantering är pålitlig ur ett användarperspektiv, undersöks de ovanstående faktorerna genom CIA-triaden. Genom att ta hänsyn till huruvida data och information hanteras i förhållande till konfidentialitet, integritet och tillgänglighet, kan vi kartlägga vilka styrkor och brister det smarta hemmet besitter. Detta är något som i slutändan kan tydliggöra eventuella åtgärder som bör vidtas för att stärka användarnas förtroende för tekniken och dess pålitlighet.

Modellen i dess helhet
Genom att undersöka samspelet av samtliga aspekter, skapar vi en förståelse för hur dessa kan påverka användaren som individ i dennes vardag. Modellen berör områden som låter oss undersöka de smarta enheternas användning och spridningen av insamlad data samt konsekvenser som uppstår genom detta. Den låter oss även undersöka och förstå systemets faktiska påverkan på användaren samt användarens uppfattning kring det.

3. Metod

I detta kapitel beskrivs hur arbetet med vår forskning genomförts, där vi tydliggör hur vi gått tillväga för att leverera relevanta, trovärdiga och faktiska resultat för hur den personliga integriteten påverkas av det smarta hemmets datainsamling. Resultaten har tillhandahållits genom en kvalitativ studie där teoretiskt och empiriskt material samlats in genom diverse litteratur, akademiska avhandlingar och artiklar samt djupintervjuer. Vårt mål har varit att genomföra forskningen med ett neutraliserat tillvägagångssätt, där personliga värderingar har undanhållits för att generera ett resultat som enbart bygger på material som erhållits via vår forskningsprocess.

3.1 Val av metod

Studiens syfte är att identifiera vad som krävs av det smarta hemmets enheter och dess tillverkare, för att indikera pålitlighet ur användarperspektiv. Vidare hoppas vi kunna öka medvetenheten hos det smarta hemmets användare och tillverkare, för huruvida den personliga integriteten påverkas av det smarta hemmets insamling och delning av data. För att kunna påvisa detta, valde vi att göra en kvalitativ studie som skapar en närhet mellan det som undersökts och oss själva (Jacobsen, 2002). Genom att utföra studien med ett kvalitativt förhållningssätt, har det låtit oss undersöka personliga perspektiv och förstå andra människors uppfattning av smarta hem (Jacobsen, 2002).

Eftersom vi försöker skapa en förståelse för och en så fullständig bild som möjligt av en situation, använder sig studien av en intensiv uppläggning. Detta gör det möjligt för oss att finna individuella variationer och skillnader i dess uppfattning och tolkning av vårt forskningsområde (Jacobssen, 2002). Med vår studie undersöker vi ett fenomen - användarens indikation av pålitligheten - och försöker kartlägga hur aspekter av vår kontext - smarta hemmets insamling och spridning av data - bidrar till denna påverkan.

"Att gå på djupet är ett försök att få fram så många nyanser och detaljer i själva fenomenet som möjligt", (Jacobsen, 2002).

Eftersom studiens fokus ligger på vårt fenomen, samtidigt som fenomenet kan belysas ur olika utgångspunkter, har vi använt oss av 'Små-N-studier'(Jacobsen, 2002). Metoden används främst på grund av att vi vill kunna gå mer på djupet med varje enskild individ, för att skapa en bättre och djupare förståelse för dennes tankar och åsikter kring vårt forskningsområde. På grund av detta, lämpar sig denna metoden bättre än exempelvis en fallstudie, eftersom vi fokuserar på vårt "fenomen" snarare än ett specifikt fall (Jacobsen, 2002)

För att se på fenomenet ur flera olika infallsvinklar användes källtriangulering. Vi intervjuade personer med olika relation till problemet - tillverkare av smarta enheter, anställda inom en svensk säkerhetsmyndighet samt användare av smarta enheter - för att erhålla en mångfacetterad förståelse för vårt forskningsområde (Mertens & Hesse-Biber, 2012). Detta gav oss möjligheten att jämföra svar från parter med ämnesrelaterad expertis och parter som enbart erhöll en fascination för teknologi, vilket visade på skillnader och jämlikheter av såväl kritiska som positiva förhållningssätt. Trots att det intensiva upplägget har varit otroligt resurs- och tidskrävande, anser vi att kvalitén av det empiriska materialet varit värt det. I förhållande till vår studie, hade en extensiv studie genererat alldeles för ytliga svar och resulterat i material som blivit alldeles för svårtolkat för önskat resultat. Därmed anser vi att det till stor del är tack vare detta metodval, som det varit möjligt att undersöka fenomenet på ett tillräckligt djup.

Eftersom det idag sker en drastisk expansion av marknaden för smarta hem, uppstår nya och fler säkerhetsrelaterade riskerna kring den personliga integriteten Bugeja, Jacobsson och Davidsson (2016). På grund av detta anser vi att våra metodval är mer gynnsamma, då de hjälper oss att undersöka hur användarna upplevde den personliga integritetens påverkan av det smarta hemmets datainsamling på ett djupare och personligare plan. En individs upplevelse av samma fenomen, kan uppstå genom flera olika förhållanden och faktorer (Statistiska Centralbyrån, 2018). Därför anser vi att ett kvalitativt metodval är gynnsamt för vår studie, eftersom det skapat möjligheten för att ställa öppna och flexibla frågor vid intervjutillfällena.

Eftersom tekniken för smarta hem verkar utvecklas snabbare än förmågan att säkerställa den personliga integriteten i samband med dem, anser vi det vara mer gynnsamt att undersöka vad vi kan identifiera för effekter, snarare än samband mellan ett större urval. Med våra metodval kan vi undersöka djupare plan av ämnet än vad en extensiv och kvantitativ forskning hade tillåtit.

Då vi samlat in material från 9 olika berörda parter, har vi erhållit tillräckligt underlag och användbart material för att utföra pålitliga analyser. Vi anser samtliga metodval som lämpliga för vår studie eftersom de hjälper oss att analysera olika material samt nå fram till ett trovärdigt och opartiskt resultat.

3.2 Urval

Målgruppen för vår studie är såväl privatpersoner som forskare och tillverkare inom ämnet smarta hem och smarta enheter. Vi har velat ta reda på om privatpersoner är medvetna om hur data samlas in, hanteras och lagras samt hur de ställer sig till redan befintlig eller ny information kring det. Intervjuerna med användarna har därför hjälpt vår studie genom att vi har förstått hur medvetenheten kring ämnet ter sig, samt om det upplevs som ett problem. Dessutom så har vi

även fått en förståelse för hur privatpersonernas definition av personlig integritet är, vilket vi anser att det kan underlätta för framtida undersökningar kring förbättringar och utveckling av tillverkarnas policyer. Detta har även hjälpt oss att se vad som har behövt förtydligas eller förbättras i den information kring datahantering som företagen tillgängliggör, i förhållandet till skydd av den personliga integriteten. Ser användarna att redan tillgänglig information är tillräcklig eller bristfällig, om detta är ett problem eller inte.

Företagsrepresentanten och personen från den svenska säkerhetsmyndigheten, har valts ut som intervjupersoner efter den information och kunskap de besitter. För att dessutom få en relativ bredd i intervjupersonernas åsikter, var vi även noga med att intervjuerna av det smarta hemmets användare inkluderade personer med olika kön och blandade åldrar. Vi anser därmed ansett att de har kunnat ge oss riklig och god information, vilket är ett av kriterierna för urval av respondenter som Jacobsen (2002) har klarlagt. För att kunna uppnå kravet bör intervjupersonerna ha god kunskap om ämnet smarta hem, kunna uttrycka sig väl samt villiga att lämna information (Jacobsen, 2002).

Intervjuperson från den svenska säkerhetsmyndigheten arbetar med data- och informationshantering online. Den intervjuade en företagsrepresentanten kommer i sin tur från en leverantör av enheter för det smarta hemmet och har bidragit till förståelse för hur den data som samlas in, hanteras och behandlas.

Vi är otroligt tacksamma över samtliga intervjuer vi fick möjligheten att hålla. Dock hade vi hoppats på att kunna hålla fler intervjuer med olika företag, men lyckades dessvärre inte hitta lämpliga respondenter som kunde medverka i intervjuer inom rätt tidsram.

INTERVJUPERSON	TYP
IPA1	Användare
IPA2	Användare
IPA3	Användare
IPA4	Användare
IPA5	Användare
IPA6	Användare
IPA7	Användare
IPFR	Företagsrepresentant
IPSS	Svensk Säkerhetsmyndighet

Tabell 1 - Sammanfattning av intervjupersonerna

3.3 Genomförande

Intervjuerna har genomförts via en dialog mellan oss undersökare och de som har blivit undersökta, där vi har spelat in och noterat vad de undersökta har sagt under samtalen. Vi hade sedan tidigare sammanställt en intervjuguide för oss själva för att kunna leda intervjun. Dock har vi försökt utveckla relativt öppna frågor och gått in med en neutraliserad tillvägagångssätt, där vi främst låtit intervjupersonen att självmant förklara sina tankar och kunskaper för undvika att leda dem mot ett svar. För att förtydliggöra har vi alltså inte använt oss utav några frågeformulärer utan istället genomfört intervjuerna med verbala meningar och berättelser för en klarhet över hur intervjupersonen uppfattar olika situationer. Dialogerna har skett ansikte mot ansikte men även via telefon. På så sätt har det inte funnits några begränsningar för vad intervjupersonen kan säga (Jacobsen, 2002). Vi har valt att genomföra intervjuerna på detta sätt då vi anser att både vi och den undersökta får ut så mycket som möjligt från intervjun och därmed har vi sedan stora mängder data att utgå från när vi bygger vidare undersökningen (Jacobsen, 2002). Informationen från intervjuerna har därför varit en förstahandskälla, då intervjupersonerna har själva deltagit i undersökningen där deras svar har varit direkt kopplat till dem (Jacobsen, 2002).

Den kvalitativa metoden tillät oss alltså närhet till intervjupersonen och har även att gett oss

flexibilitet och en djupare förståelse genom att observera intervjupersonen. Dessutom har vi valt en individualistiskt ansats för att minimera beroendet av sociala sammanhang (Jacobsen, 2002).

Det fanns goda möjligheter för oss att hitta teoretiskt material via internet. Vi har lagt störst fokus runt internationella företag som har kontor i Sverige, samt studier som fokuserar på den personliga integriteten, datainsamling och behandlingen av data. Dessa källor har kunnat bland annat ge oss värdefull information kring hur smarta hemmet påverkar den personliga integriteten. Hemsidor som Google Scholar och LU:s- söksystem har används som sökmotorer för att kunna hitta relevanta artiklar och övrigt material för vår studie.

Fokus har legat på att undersöka vetenskapliga rapporter samt vetenskapliga studier som har berört vårt ämne. Vi har även tagit hänsyn till olika aspekter samt krav som ställs av nationella myndigheter och organ. Sedan har vi bland annat undersökt övriga rapporter, vetenskapliga artiklar samt vetenskapliga tidskrifter som har berört vårt ämne.

3.4 Datainsamling

Vid studiens start hade vi väldigt snäv kunskap om hur smarta hemmets enheter samlade in och hanterade information. Detta ledde till att vi gjorde en induktiv ansats (Jacobsen, 2002), där vi påbörjade forskningen utan några förväntningar och försökte samla på oss material som var relevanta för vår studie. Vid val av material, lade vi stor vikt på att kolla författarnas bakgrund, se så att nyckeltalen stämde överens med våra egna och var källkritiska genom att undersöka vilka metoder som har använts i de tidigare forskningar.

Data som har samlats in har bland annat varit statistik, bedömningar och resultat från tidigare forskning inom liknande forskningsområde som vi undersöker. Vi har även tittat på användarvillkor, som jämförts med vårt empiriska material som samlats in genom intervjuer av de smarta enheternas användare, tillverkare samt en svensk säkerhetsmyndighet. Vi har hittat och samlat in materialet genom digital och fysisk litteratur, där sökorden har baserats på våra nyckelord.

Vi har bland annat valt att använda webbsidor som har varit utformade av företag som Google och Apple. Anledningen till varför vi har valt att undersöka dessa webbsidor är på grund av att de är företag som är leverantörer av enheter för smarta hem (IoT). Vi har även valt att använda oss utav webbsidor där tidigare forskningar har gjorts av eller berör vårt forskningsområde. Dessa webbsidor har bland annat innehållit teorier och forskning kring big data, data analytics, Internet of Things, molntjänster, smarta hem, användares förståelse av användarvillkor, datainsamling och datahantering. Denna typ av material har bland annat samlats in och använts för att förstå hur det smarta hemmet och dess beståndsdelar är tänkt att fungera, för att sedan se

och jämföra hur det faktiskt ser ut hos företagen idag med användarnas åsikter kring vad som förväntas av en pålitlig smarta-hem-enhet.

3.5 Intervjuguide

Vi har valt att skapa tre olika intervjuguider för att kunna få ut så mycket som möjligt ur våra intervjuer, eftersom att intervjupersonerna har haft olika roller i vår studie. Det har alltså gjorts varsin intervjuguide för användarna, företaget och den svenska säkerhetsmyndigheten, för att kunna ställa relevanta frågor och få relevanta svar från olika perspektiv.

Intervjuguiderna baseras främst på IoT-teorin och CIA-modellen, för att kunna nå fram till en slutsats som har följt en röd tråd. Vi anser att detta har varit viktigt för att kunna basera vår diskussion och slutsats på resultat som går att jämföra och analyseras med vår teori och modell. Vi har valt att endast fokusera på dessa två teorier och modeller i våra intervjuguider eftersom vi ansåg dem vara mest tillämpbara för vår forskningsfråga och studie. Eftersom att forskningsfrågan riktar sig mot ett användarperspektiv, har vi valt att fokusera främst på användarnas resultat för att se hur de uppfattar pålitligheten i ett smart hem-system. Vi har därför inte tagit med alla frågor i resultat- och diskussionsdelen som finns med i intervjuguiderna för IPFR och IPSS eftersom vi inte anser att alla frågor måste tas upp där. Dock har vi kvar frågorna i intervjuguiderna för att ge läsaren en helhetsbild av hur företagen arbetar med datainsamling och datahantering.

CIA-modellen har valts för att förstå användarnas pålitlighet kring hur deras data hanteras och behandlas. Intervjuguiderna är även baserade på IoT-lagren för att kunna förstå hur den data som samlats in, hanterats och behandlats kan påverka den personliga integriteten när data utsätts för i olika miljöer som eventuellt kan göra den sårbar. Eftersom att våra intervjupersoner har valt att vara anonyma i intervjuerna, har vi gett dem pseudonym-beteckningar för att presentera deras resultat.

3.6 Dataanalys

Analysering av data är en betydelsefull process för själva undersökningen och Jacobsen (2002) har framtagit tre steg som ger en effektiv metod att kunna analysera data i en kvalitativ undersökning. Dessa stegen är: *beskrivning, systematisering* och *kategorisering samt kombination*. Stegen bör göra det enkelt för författarna att analysera och hantera sin data på ett strukturerat arbetssätt samt för att minska den komplexitet som kan förekomma i en kvalitativ undersökning. Dessutom ger det en överblick av den information som har samlats in, vilket bidrar till en effektiv analyseringsmetod (Jacobsen, 2002).

Beskrivning

I detta steg gäller det att få en grundlig och detaljerad beskrivning av den data som har samlats in genom att ha registrerat situationer, intervjuer och samtal så noga som det går (Jacobsen, 2002). Genom att vi både har antecknat och spelat in intervjuerna som har inträffat, har vi anträffat detaljer som annars hade kunnat förbisetts.

Efter varje intervju har vi diskuterat och jämfört våra anteckningar för att kunna sammanfatta vår data och våra tankar. Vi anser att vi har därför kunnat analysera på djupet och hitta olika variationer i vår data som har gett oss det Jacobsen (2002) benämner som *tjocka beskrivningar*.

Systematisering och kategorisering
Nästa steg blir att systematisera och kategorisera den information som har samlats in. Det sker genom sållning och förenkling av information för att kunna få en överblick av materialet. Jacobsen (2002) menar att systematisering och kategorisering är viktigt för att kunna förmedla vad författarna har funnit. Vi valde att efter varje intervju sortera och kategorisera den data som vi hade samlat in för att enkelt kunna sammanställa den.

Kombination
När de föregående stegen har genomförts kan tolkningen av data påbörjas, vilket innebär att vi har letat efter meningar, motiv och generaliseringar. Ett av våra mål har varit att försöka hitta dolda och intressanta förhållanden (Jacobsen, 2002), vilket bland annat möjliggjorts genom att jämföra det empiriska och teoretiska materialet som samlats in. Genom att använda oss av källtriangulering, blev det även möjligt för oss att se på vårt problemområde ur olika perspektiv, vilket hjälpte oss i arbetet att försöka hitta givande resultat och dra relevanta slutsatser.

3.7 Etik

Enligt Jacobsen (2002) kan det vara bra att dölja avsikten med en undersökning för att de intervjupersonerna inte ska känna sig hotade. Det är ett naturligt beteende som människor framträder när det vet att de blir studerade. Dessutom kan personerna uppträda annorlunda än vad de hade gjort i en vanlig situation.

Jacobsen (2002) nämner tre anledningar som finns till detta beteende:

- De vill inte avslöja sitt sanna jag
- De vill tillfredsställa undersökaren
- De vill framstå på ett annat sätt

Vi har försökt motarbeta detta beteende genom att försöka skapa en naturlig miljö för den undersökta samt inte få dem att tro att vi vill höra ett specifikt svar. För att inte påverka eller leda de intervjuade individerna åt ett specifikt håll, har vi därför valt att ställa frågor med ett

neutraliserat förhållningssätt. Vi har även själva valt att se på vårt forskningsområde med en neutraliserad synvinkel, där vi inte beblandar personliga åsikter i vår forskning och enbart baserar analys och resultat på forskningsmaterial.

För att intervjutillfället ska vara så etiskt som möjligt har vi valt att arbeta med tre grundkrav som Jacobsen (2002) har sammanställt i tre punkter:

1. Informerat samtycke
Intervjupersonen ska ha frivilligt deltagit i vår undersökning och det har inte funnits något tvivel på att den som har undersökts inte kan värdera fördelar och nackdelarna med att delta och sedan göra ett val. Den undersökta ska ha förstått hela syftet med undersökningen och har fått all information kring det.

2. Rätt till privatliv
Intervjupersonerna har kunnat avstå från att svara på frågor som de inte är bekväma med att svara på, vilket inkluderar privata frågor och känslig information som kan komma att skada verksamheten för det smarta hemmets enheter.

3. Krav på riktig presentation av data
Den insamlade datan har spelats in och transkriberats för att läsaren och intervjupersonerna ska få se resultatet i ett fullständigt samt rätt sammanhang. Riktig presentation av data innebär också att data inte får förfalskas, vilket vi anser vara en viktig regel att följa i en undersökning. För att undvika detta har vi exempelvis skickat transkriberingen av utförd intervju till intervjupersonen och låtit de läsa texten för att kontrollera om den överensstämmer det som sagts. Vid eventuella invändningar från intervjuperson har dessa beaktats, tagits hänsyn till och resulterat i mindre korrigeringar.

Under studiens gång har vi även lagt stort fokus vid att eliminera alla former utav plagiat, där vi värdesatt uppvisandet av verklig författare bakom den information som granskats och integrerats i uppsatsen. För att undvika plagiering, har vi arbetat med Bui's (2009) tre ledord i åtanke genom hela uppsatsen.

1. Utför ditt eget arbete.
2. Ge beröm till den verkliga källan för såväl idé som information och data.
3. Skriv om meningar som använts från källor istället för att kopiera dem rakt av.

Genom att gå efter dessa ledord har vi kunnat leverera ett faktabaserat och trovärdigt resultat utan att presentera ett stulet och redan befintligt arbete (Bui, 2009).

3.8 Validitet och reliabilitet

Genom att grunda våra intervjufrågor på det teoretiska ramverket som vi har presenterat har vi på så vis stärkt undersökningens validitet. Dessutom har vi även kunnat styrka validiteten i vår studie genom att få intervjua personer med olika roller inom det smarta hemmet och på så vis fått fram resultat med olika infallsvinklar, vilket har hjälpt oss att analysera och jämföra material med och mot varandra. Genom detta har vi kunnat kritiskt granska själva resultaten (Jacobsen, 2002) och kunnat hitta direkta och indirekta kopplingar som har hjälpt oss att nå fram till en slutsats som är trovärdig.

Då studiens syfte är att förstå vad som indikerar pålitligheten ur ett användarperspektiv har vi därför framförallt intervjuat flest användare, där vi har kunnat hitta liknande resultat bland intervjupersonerna och resultat som även indikerar att den teorin och modell som har vi presenterat och tolkat är av relevans.

Vi har alltså gjort en intern kontroll för om vi har kommit fram till rätt resultat och slutsats på ett riktigt sätt. Sedan har det även gjorts en extern kontroll för om undersökningen kan generaliseras. För att kunna generalisera svaren, har vi bland annat valt intervjupersoner i olika åldrar.

Då vi har haft fysiska möten samt intervjuer över telefon, har intervjupersonerna kunnat korrigera sina svar direkt om de så ansåg att det behövdes. Enligt (Jacobsen, 2002) är det viktigt att mäta hur pass forskningen är utav reliabilitet och där Jacobsen (2002) förklarar att intervjuernas miljö får en viss påverkan på intervjupersonens svar. Vi har därför låtit intervjupersonerna bestämma vilken tid och plats intervjuerna ska hållas. De flesta intervjuerna har hållits per telefon, vilket också reducerar en viss påverkan på intervjupersonens svar där hen kan ha blivit påverkad över vår närvaro och till exempel över hur vi har klätt oss.

Sedan förklarar Jacobsen (2002) att finns det en annan risk med att de som intervjuar inte uppmärksammar svaren som intervjupersonerna ger under intervjuernas gång, vilket kan leda till att de som intervjuar missar viktiga ståndpunkter (Jacobsen, 2002). För att undvika detta har vi tillfrågat intervjupersonerna ifall vi får spela in intervjun, vilket de har gått med på. Detta har tillåtit oss att kontrollera svaren från intervjupersoner genom att skicka transkriberingen till dem i efterhand.

4. Resultat

I detta avsnitt presenteras våra intervjupersoners svar. Avsnittet har delats upp i fem olika sektioner, där vi kategoriserat in intervjuernas resultat utefter relevant rubrik.

1. Enheternas pålitlighet

Litar användarna på det smarta hemmets system?

Figur 5 - Användarnas förtroende för de smarta enheternas kommunikation

För att förstå hur användarna ser på den datainsamling som sker via smarta enheter, frågade vi de intervjuade användarna hur de ställde sig till att de smarta enheterna samlar in data från dem. Det visade sig att 71% av de intervjuade användarna ansåg att det inte var okej med att deras data användes för ett annat ändamål än enhetens syfte eller att det delades med andra enheter.

När vi sedan frågade samtliga användare om de litade på den överföring som sker mellan enheterna samt mellan enheterna och företagens servrar, svarade 86% att det finns en brist i förtroendet. 14% svarade att de litade på dataöverföringen, men att det däremot fanns en oro för att de smarta enheterna skulle kunna bli hackade. En stor grund till varför det finns ett avsaknat förtroendet verkar vara en konsekvens från alla nyheter som ständigt flödar om hackers och nya

dataläckage. IPA4 förklarar hur den enda slutsatsen som kan tas från den information som hen hittar och ser på nyheterna, är att inget system är helt säkert.

IPFR pratade dock om hur företaget, där hen arbetar på, jobbar med att skydda den personliga integriteten genom bland annat krypteringsstandarder. Detta ledde oss till frågan om all data som deras system behandlar, också skyddas av krypteringsstandarder, inklusive lösenord och videoströmmar etcetera. IPFR bekräftade att det ska göra det och följdfrågan blev då om all data som samlas in genom de smarta enheterna behandlas likadant, där IPFR svarar "Ja.". Svaren på frågorna tydde på att företaget som IPFR arbetar på, jobbar mycket med att försöka uppnå kvalitet säkerhet i sina produkter.

För att förstå hur företaget där IPFR arbetar på, arbetar för att skydda deras användare, frågade vi hen om det finns några slags behörighetskrav för de anställda, som begränsar eller ger dem tillgång till den data som samlas in från de kameror som de säljer. IPFR svarade att hen inte vet vilka eller om det finns några behörigheter för de anställda men att kamerorna har själva någon slags begränsning, där en liten lucka slås på så fort en användare kommer hem. Detta ska på så vis skydda privatlivet genom att endast spela in, när familjemedlemmarna inte är hemma.

Vidare berättar IPA4 även hur hen fått intrycket av att vilket system som helst kan bli hackat om det finns någon som vill göra det tillräckligt mycket och är någorlunda duktig. Lyssnar vi på IPA3 kan vi se hur en viss grad av detta antagande och oro kan bekräftas. Under intervjun berättade IPA3 att en kontakt till hen arbetar som en CEH för företag och besitter förmågan att kunna bryta sig in i någons bank och rensa kontot. Det enda som IPA3's kontakt behövde var offrets mobil, vilken hen ansåg sig kunna hitta tillräckligt med information från för att generera en lyckad attack i offrets mobilbank vid 99% av fallen. Detta tyder på att om en person har tillräckligt kunskap om programmering och ett motiv för att hacka någon, är det möjligt att komma åt känslig information i majoriteten av fallen. IPSS påpekar hur hackare alltid ligger steget före, eftersom deras jobb går ut på att hitta säkerhetshål i systemen. Dock förklarar hen samtidigt hur viktig användarens lösenordshanteringen är, för att minimera risken för intrång i dess smarta enheter. När vi sedan frågade IPSS om hur lång tid det tar innan individer eller företagen upptäcker intrång på nätverket, svarade hen att det är svårt att avgöra på grund av det stora mörkertalen av offren. Hen förklarade dock hur företag brukar vara snabba på att stoppa intrång när de väl ser det, men fortsätter att förklara hur det dessvärre inte är så många företag som anmäler intrånget till polisen ifall de blir utsatta för det, eftersom det skapar dålig reklam för företaget.

"Det är många som inte anmäler och det är även företag som inte heller anmäler även fastän de har blivit utsatta för att det är, ja dålig reklam för dem att de har blivit hackade [...]" - IPSS, Personlig kommunikation, 2 maj 2018

För vissa av de intervjuade användarna, grundar bristen av förtroende även på egna erfarenheter. IPA2 berättar bland annat hur någon annan, okänd, användares bilder kommit in i hens moln av misstag. Vidare förklaras den efterföljande oron från IPA2 kring vem som kan tänkas ha fått hens egna bilder av misstag samt sannolikheten för att denna typ av brist vid filöverföring över molnet, troligen kan ske vid överföring av annan data också. Även IPA3 har egna erfarenheter där tekniken brustit vid överföring av data och information. IPA3 berättar hur hens kontroll för sina smarta enheter i hemmet, vilket hanterades via en app i mobilen, helt plötsligt hade förändrad vy och plockat upp någon annans styrsystem för dennes smarta enheter i sitt hem. IPA3 berättar hur hen inte var särskilt imponerad över att misstag som detta var möjligt att ske, eftersom det kan vara känslig data som hanteras i de smarta enheterna i hemmet. Vidare berättar hen att om problemet skulle uppstå fler gånger eller regelbundet, skulle det förmodligen resultera i att hen slutar använda de smarta enheterna eftersom det äventyrar säkerheten för den personliga integriteten.

När de intervjuade användarna tillfrågades ifall de litade på att de smarta enheternas system fungerar som de ska, indikerade samtliga att det inte fanns ett hundraprocentigt förtroende för enheternas system. 43% av de tillfrågade nämner dock hur de ändå försöker lita på systemet, eftersom de känner att de inte har något annat val ifall de vill använda det. IPA2 förklarar hur hen upplever att system ofta används av samhället, trots att det inte finns tillräckligt mycket underlag för att kunna säkerställa att systemen verkligen fungerar som de ska. Majoriteten av användarna antydde även medvetenheten om att risken för brister i systemet alltid finns eftersom det trots allt rör sig om teknik. Däremot visade 100% av de tillfrågade en positiv attityd gentemot de smarta enheterna uppträdande rent funktionsmässigt inom sitt tänkta användningsområde.

"Du måste vara ganska duktig själv på tech och grejer för att kunna förstå och begränsa de här enheterna för att göra som du vill och kan förstå riskerna med det. Förstår du inte detta, så tror jag det kan vara väldigt väldigt enkelt att utnyttja." - IPA7, Personlig kommunikation, 4 maj 2018

När vi intervjuade användarna och frågade ifall de upplevde någon risk för manipulation av data, svarade samtliga att det finns en definitiv risk för det. IPA7 förklarar bland annat hur hen anser att användare alltid löper en risk för att få sin data manipulerad. Vidare förklarar hen även sina tankar eventualiteten att tekniskt okunniga riskerar att löpa större risk för att omedvetet utsättas för manipulation av data från obehöriga parter och därmed utnyttjas. Detta eftersom att om användaren har en bristande förståelse för hur tekniken fungerar, har den förmodligen inte heller kunskapen om hur eller att den ens behöver skydda sig från det.

2. Otydlig data

Har användarna försökt ta reda på vilken information som samlas in, hanteras och lagras? Vet användarna vilken information som samlas in, hanteras och lagras?

Figur 6 - Användarnas försök att hitta information

När vi intervjuade användarna, försökte vi ställa frågor som indikerade på om de försökt ta reda på företagens tillvägagångssätt för att samla in och hantera information genom de smarta enheterna. Detta gjordes för att kunna skapa en relativ förståelse till varför de intervjuade användarnas åsikter såg ut som de gjorde, i förhållande till företagens informationshantering av de smarta enheternas insamlade data. Efter att ha sammanställt resultaten har vi kunnat konstatera att endast 29% av de tillfrågade gjort ett försök till att ta reda på vilken information som samlas in om dem. Av de tillfrågade var det, även här, endast samma 29% som hade försökt ta reda på hur informationen hanterades eller lagrades. Vi frågade även IPSS om det är betydelsefullt för konsumenten att tänka på vilket företag de köper sina produkter från och vad de säger med sina användarvillkor samt säkerhetspolicy. Hen svarade då att villkoren och policyer är alldeles för komplicerade, vilket innebär att det är för mycket jobb att läsa igenom dem. Användare kan därför bli otåliga, vilket resulterar i att det är nästan ingen som läser igenom villkoren och policyer.

"Ja det beror ju på vad man ska köpa in och ser man till gemene man så är det ingen som läser

de här policyer eller villkoren och det blir för komplicerat och det blir för mycket jobb." - IPSS, Personlig kommunikation, 2 maj 2018.

Figur 7 - Orsaker till användarnas val att inte leta efter information

När vi frågade varför övriga inte gjort någon som helst ansträngning till att ta reda på detta, svarade samtliga av de tillfrågade att de antingen har varit för lata, inte brydde sig eller inte hade någon aning om vart de ens skulle vända sig för att få åtkomst av sådan information.

"Man döljer ju saker och ting lättast helt öppet för då dränker man ju den informationen i en textmassa så att det är väldigt svårt att hitta den texten man kanske då är intresserad av." - IPA1, personlig kommunikation, 29 april 2018.

Efter att ha studerat och jämfört användarnas intervjuer, verkar okunskapen och "latheten" vara konsekvensen av att användarvillkor och säkerhetspolicyer känns alldeles för långa och komplicerade för att ta sig igenom och förstå. Arbetsbördan för detta upplevdes helt enkelt som för stor. IPA2 svarade att det fanns en känsla av maktlöshet vid tanken på att försöka ta reda på denna typ av information. Orsaken till detta ställningstagande var hens uppfattning om att företagen inte utformade dessa avtal med hänsyn till användaren, utan främst för att de ska kunna hålla ryggen fri från ansvar vid eventuella komplikationer. Majoriteten av de tillfrågade trodde att det fanns en definitiv baktanke till den långa harang av text som ofta förekommer i användarvillkoren. Den främsta orsaken till denna typ av utformning, ansågs vara ett sätt för företagen att kunna dölja textens verkliga betydelse och därmed få användaren att acceptera saker slentrianmässigt, genom att göra det önskade innehållet svåråtkomlig och därmed trötta ut användaren.

En annan orsak till varför användarna valde att inte läsa användarvillkoren, verkar grunda sig i dess öppna och komplicerade formuleringar. Språket som används uppfattades i flera fall som svårtolkade för användare med en icke-teknisk bakgrund och meningarna ansågs ha en alldeles för fritolkande och öppen verbalisering.

"[...]de använder sig utav variabler som man själv inte förstår och då tar det flera timmar att sätta sig in i det och sen tar det ytterligare flera timmar att förstå konsekvenserna senare." - IPA5, personlig kommunikation, 5 maj 2018.

Av de 29% som försökt ta reda på vilken information som samlas in och hanteras, var det 100% som valde att avbryta sitt sökande av denna typ av information eftersom de ansåg att informationen var alldeles för svår att hitta och för komplicerad att tolka . IPA5 nämnde i sin intervju hur hen upplever att försök till åtkomst av denna typ av information är en krånglig process och förklarar hur företagens hemsidor och sökfunktioner inte känns användarvänliga. Vidare förklarar IPA5 hur informationen var utspridd på flera olika sidor från samma företag, något som upplevts som förvirrande och frustrerande. Detta är en aspekt som tyder på hur användarna upplever eftersökt information som svåråtkomlig, där inte ens försök att ta reda på dem känns tillräckliga ifall användaren inte vill spendera en orimligt längre tid på att söka och försöka förstå innehållet.

Även IPSS ansåg att företagets villkor och säkerhetspolicyer var för komplicerade och innebar för mycket jobb att gå igenom, när vi frågade hen om det är värt för användare att tänka på vilket företag de köper deras smarta enheter från och vad de säger med sina säkerhetspolicyer. När vi frågade IPSS vilken den största orsaken för identitetsstölder är och om det finns något mönster bakom det, svarade hen att användare ofta är väldigt slarviga med sina lösenord för att de inte anser sig själva vara i riskzonen för sådana situationer. IPSS förklarar att användarna istället tycker det är jobbigt att behöva byta lösenord på två konton och att de istället väljer att ha samma lösenord för att de inte förstår riskerna och hur lätt det är för hackare att ta det av information som "folk bara släpper ifrån sig".

3. Företagens datahantering

Litar användarna på företagen? Är vinsten större än risken i förhållande till de smarta enheternas informationshantering?

När vi frågade de intervjuade användarna ifall de visste vilken information som samlades in om dem, kunde vi se ett mönster, där majoriteten var medvetna om att de smarta enheterna samlade in data om dem. Dock blev det ganska snabbt tydligt att majoriteten däremot inte hade någon större kunskap om vilken den exakta data var som samlades in. En stor orsak till användarnas medvetenhet om informationsinsamlingen, verkar vara den individualiserade marknadsföringen som uppkommer i samband med användning av de smarta enheterna.

"Nej jag har inte försökt kolla upp det, utan det liksom har man väl märkt bara." - IPA2, personlig kommunikation, 29 april 2018.

Figur 8 - Användarens uppfattning om datainsamlingens syfte

På frågan om användarna ansåg att företagen samlade in data och information främst för sitt eget eller användarens syfte, missade vi tyvärr att ställa frågan till 14% av dem. Av de tillfrågade var det dock 100% som trodde att företagen använde den insamlade data och informationen, främst

till företagets egna syfte och inte användarens. Även IPSS förklarade hur utformandet av företagens användarvillkor kan vara en orsak till att möjliggöra ett så stort informationsintag som möjligt av användaren, för att kunna individanpassa produkter och marknadsföring. Hen förklarar även att det egentliga ansvaret ligger på användaren, eftersom accepterande av användarvillkor ofta ger företagen full åtkomst av exempelvis kameror och kontakter. Samtidigt nämner hen även hur godkännandet av villkoren fungerar enkelriktat, där ett accepterande av företagens vilja och krav är det enda valet användaren ges ifall de vill använda produkten.

För att förstå företagens sätt att hantera eventuella risker kring ofrivillig spridning av kunddata, frågade vi IPSS hur lång tid det tar för företagen att upptäcka intrång på deras nätverk. Hen svarade att företag oftast har en övervakning och säger att *"De sitter och kollar vilken information som är på gång på deras nätverk, så de har ju verkligen hängslen och livrem så de ser ju till att stoppa det på en gång."*. Vidare berättar hen att det oftast går fort att upptäcka en sådan händelse eftersom företagen ofta är måna om att skydda sin data. Däremot påpekar hen att statistiken är ett mörkertal, då de flesta företag inte anmäler dessa intrång eftersom det skulle ge dem dålig reklam att de har blivit hackade.

4. Datas förmåga att påverka

Hur ställer sig användarna till att de smarta enheterna samlar in data om dem?

Figur 9 - Användarnas åsikt kring datainsamling

När vi frågade de intervjuade användarna om hur de ställer sig till att de smarta enheterna samlar in data om dem, var det 71% av de tillfrågade som inte ansåg sig bekväma med detta ifall datainsamlingen inte stannar inom ramarna för de mottagare som de själva anser är godkända.

"Om de samlar in data om mig som är tillgänglig endast för mig då är det okej, men om de samlar in data som obehöriga kan få tillgång till då tycker jag inte att det är okej." - IPA5, personlig kommunikation, 5 maj 2018.

De övriga 29% av de tillfrågade tyckte fortfarande inte att det var okej att de smarta enheterna samlade in data om dem, ifall den även skulle användas av tredje part eller till ett annat ändamål än det vad produkten egentligen var till för. Däremot hade de accepterat insamlingen av data för att antingen kunna få använda produkten eller för att de ansåg att det fanns olika grader av acceptans beroende vilka områden som verksamheten valde att använda datan inom och till vad, när det gällde deras personliga datainsamling.

"Jag skulle väl säga att jag är mer positiv till det än många andra. Av anledning till att jag tycker det är rimligt att viss typ av aktivitet som man gör på internet eller gör någon annanstans är väldigt öppen och borde samlas in. [...] Dock så tycker jag att information som samlas in om en, som man inte är tydligt medveten om att den samlas in, den tycker jag liksom inte riktigt är okej." -IPA7, personlig kommunikation, 4 maj 2018.

IPA7 förklarar att hen inte såg det som något problem om enheten skulle samla in data från personen till för att skräddarsy reklam för hen, eftersom det inte skulle påverka den personliga integriteten i det mån att personens uppgifter endast används för viktiga och transparenta aktiviteter. Men så fort datainsamlingen skulle ske bakom stängda dörrar, där användaren inte är medveten om hur den hanteras, då är det inte längre ett acceptabelt tillvägagångssätt. Dessutom är det ett faktum att om användaren inte accepterar användarvillkoren, så kan de inte använda sig utav enheten, fastän användaren inte vet vilken data de samlar in.

"That's what I've bought in to. But I don't know what data they collect, it must all be done by, I'm not sure how it works really." - IPA3, personlig kommunikation, 30 april 2018.

Samtidigt som alla de intervjuade användarna är överens om att det inte känns bra att företagen samlar in data om dem, berättade IPFR att de får allt fler frågor kring hur de hanterar deras användares data. Om det är en effekt från Facebook-skandalen, eller att människor har blivit alltmer medvetna, är inte säkert men det går att konstatera utifrån vår forskning att den personliga integriteten blir alltmer viktigt eller upplyst för användarna.

"[...]och inte att förglömma naturligtvis, kameror i hemmet, vilket verkligen anspelar på den personliga integriteten, kan man säga." - IPFR, Personlig kommunikation, 20 april 2018

Resultaten antyder på att frågan kring hur användarna ställer sig till att de smarta enheterna samlar in data om dem, blir allt viktigare ju mer det anspelar på den personliga integriteten. Vilket är något IPFR har märkt av, då de har fått en hel del frågor om säkerhetsaspekten kring den personliga integriteten. Det är även något som IPFR har försökt vara tydlig med under intervjun, där hen förklarar att användarna inte behöver lämna ifrån sig så många personliga uppgifter när de använder deras produkter, där främst mailadress och lösenord krävs. IPFR förtydligade även att det inte krävs några personnummer för att ansluta sig till deras system.

5. Rädsla kontra fördelar

Vilken data anser användarna vara mest känslig i förhållande till säkerhet av deras personliga integritet?

Vad är din definition av personlig integritet? Frågan ställdes till alla de intervjuade användare för att förstå vad deras definition är och vad de tycker är extra viktigt när det kommer till den personliga integriteten. En gemensam tråd för samtliga, var åsikten om att den personliga data som samlats in om dem, endast bör stanna inom de ramarna som användarna själva velat och varit medvetna om att de godkänt. För att få ett annat perspektiv, ställde vi ställde samma fråga till IPSS för att förstå hur hens definition av begreppet såg ut. Hen svarade att det är en klurig fråga, men att det gäller den data som användare lämnar ut och vilka fler som får tillgång till den information, samt möjligheten till att bygga ihop denna information så att den kopplas tillbaka till användaren.

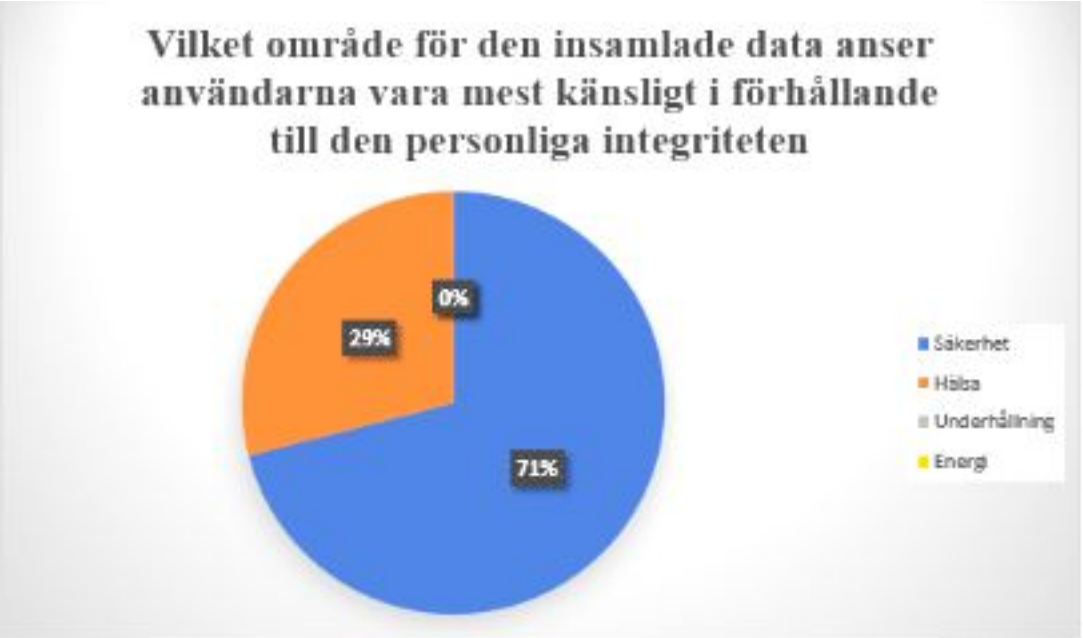
När de tillfrågade fick svara på frågan ifall de ser några risker för den personliga integriteten vid användning av smarta enheter, var det 100% som svarade att de ansåg att det fanns risker som skulle kunna uppstå när de har smarta enheter i hemmet. Vidare frågades om vilka risker de ansåg skulle kunna inträffa i förhållande till säkerheten av den personliga integriteten och då svarade alla intervjuade användare att det fanns risk med att obehöriga skulle kunna hacka sig in i systemet. Fler utav de intervjuade användarna ansåg att det fanns risker med att företagen skulle kunna missbruka användarnas data genom att exempelvis dela med sig utav den med tredje part eller kartlägga en person fullständigt och deras beteende.

"De är väl att företagen kanske använder mina uppgifter för andra ändamål än vad min enhet är tillför, eller då såklart att min kära hackare går in och tittar på mig eller ser och säljer min data eller någonting sånt där." - IPA6, personlig kommunikation, 5 maj 2018.

Enligt IPFR medföljer konsekvenser när användare godkänner avtal med företag, där användare exempelvis tillåter företag att vidta åtgärder som en användare inte är riktigt bekväm med. För att förtydliggöra detta, ger IPFR ett exempel om en situation där ett brandlarm plötsligt börjar tjuta när en användare står och steker för att det bildas mycket rök. Då skulle larmcentralen ha möjligheten till att gå in och kolla i kameran för att se om en brand faktiskt har brutits ut, vilket egentligen kanske inte hade varit riktigt nödvändigt i det fallet. IPFR påpekar att de har haft flera kunder som ogillat en sådan handling och därför ställt frågor till dem om hur de själva, som företag, hanterar sådana situationer. Vidare nämner IPFR att även om företaget inte ska gå in och kolla i kameran utan specifik anledning, så har användaren trots allt godkänt användaravtalet som innebär att företaget har rätt till att kolla kameran när systemet utbryter eventuella larm och varningssignaler.

"[…] även om man skulle kunna gå in och kolla på kameran så får man inte lova att göra det. I det fallet får du ju göra det och då har du ju signat off för det i vad ska man säga i de legala dokumenten som du skrivit i när du har köpt systemet." - IPFR, personlig kommunikation, 20 april 2018.

Även IPSS anser att ansvaret delvis ligger på användaren, där de bör läsa igenom användarvillkoren innan de börjar att använda sin smarta enhet. Vi frågade därför IPSS om företagen gör det tillräckligt tydligt för användare om vilken data som hanteras, där hen svarade *"Både och. Samtidigt så vill de ju få in så mycket information som möjligt om användaren"*. Vidare förklarar hen att ansvaret ligger därför på användaren att läsa igenom användarvillkoren för att veta vad som sker med deras data. Samtidigt påpekar hen också att det egentligen inte gör någon skillnad att läsa igenom användarvillkoren då det inte går att installera appen om användaren inte godkänner villkoren.



Figur 10 - Användarens åsikt om det smarta hemmets mest känsliga område

Enligt resultaten går det att konstatera att det oron, att någon ska utnyttja den data som de smarta enheterna samlat in om sina användare, finns där. I intervjuerna av användarna bad vi dem välja ett av de smarta enheternas fyra områden som de upplevde som mest känsligt i förhållande till deras personliga integritet i hemmet. De fyra områdena de kunde välja mellan var *säkerhet*, *hälsa*, *underhållning* eller *energi*. Detta gjordes för att förstå vilken typ av data användarna ansåg vara mest känsligt i förhållande till säkerheten av deras personliga integritet i hemmet. Av de tillfrågade användarna svarade 71% säkerhet. IPSS berättar i sin intervju hur all data som är kopplad till individer kan klassificeras lika känslig, men antydde dock att data som kan kopplas till säkerhetsområdet kan vara extra utsatt.

"Ja det ser jag. Ja framför allt typ när det är kameror i hemmet, där det är många som är filmade och det går ut på nätet. Och det är inte säkert dem som är i hemmet som vill det." - IPA2, personlig kommunikation, 29 april 2018.

Vidare svarade 29% av de tillfrågade användare att de ansåg att data om deras hälsa är känsligast. När vi sedan frågade varför de ansåg att hälsan var mest känsligt, svarade en utav dem med ett exempel om att användaren kan bli väldigt blottad med exempelvis sin aktuella sjukdomstillstånd om de smarta enheternas leverantör delar användarens data till andra företag om vilka mediciner hen tar.

"Ja smarta enheter, smarta funktioner i alla fall. Så att så är det ju i alla fall. Att man inte använder vissa." - IPA1, personlig kommunikation, 29 april 2018.

För att se om de risker som nämndes påverkade användarnas val av vilka smarta enheter de väljer att använda sig utav, frågade vi även de intervjuade användarna om detta. 43% svarade att det inte hade påverkat deras val av vilka smarta enheter de använde sig utav i nuläget och 43% svarade att de potentiellt skulle kunna sluta använda sig utav dem, men gör det inte just nu. Sedan var det 14% av de tillfrågade användarna som svarade att dessa risker påverkar deras val med att använda sig utav vissa enheter.

För att förstå varför de intervjuade användarna fortsätter att använda sig utav de smarta enheterna trots de risker som de hade nämnt, frågade vi om de anser att vinsten är större än riskerna. Majoriteten svarade ja på denna fråga och resten svarade att de egentligen såg det som att de blir mer eller mindre tvingade till att använda sig utav de smarta enheterna.

"Nej egentligen är det ju att jag använder, man använder ju internetbanker eftersom det inte finns några vanliga banker längre haha." - IPA4, personlig kommunikation, 1 maj 2018.

"Jag tror att jag använder det vidare för att man orkar inte ta steget ur det, för att det här använder alla mer eller mindre." -IPA2, personlig kommunikation, 29 april 2018.

Vi frågade IPSS om det är viktigt ur ett företagsperspektiv och kundperspektiv att använda sig utav behörigheter i system, vilket IPSS ansåg vara viktigt för att som företag in ha tillgång till all den känsliga information som de samlar in. Hen förklarar vidare att anställda inte bör ha tillgång till samma data vilket även ger en trygghet till de anställda inom företag, och ju mindre de vet desto mindre går det att läcka.

"Arbetar man inte inom det området så behöver man inte ha en access gentemot den data heller. Så det är ju en trygghet både för personal som ja, eller anställda inom företag. Ju mindre du vet desto mindre kan du ju läcka också " - IPSS

5. Diskussion

I detta avsnitt diskuterar och jämför vi den empiriska data som samlats in under intervjuerna med den teori som presenterats i kapitel 2. Avsnittet startar med en inledning och fortsätter därefter med den kategorisering som gjordes av resultaten i kapitel 4, för att göra koppling mellan resultat och diskussion tydlig för läsaren.

Resultaten från vår studie tyder på att majoriteten av det smarta hemmets användare är medvetna om att data samlas in av de smarta enheterna som används i hushållet. Däremot finns en okunskap och ibland nonchalans för den faktiska mängden och exakta data som samlas in, samt hur bred spridningen av den egentligen är. I dagens samhälle råder samma okunskap och nonchalans för datahantering på flera håll, där majoriteten av de sociala mediernas användare villigt delar med sig av detaljerad information om deras privatliv med vänner och främlingar (Molina-Markham et al. 2010). Oftast krävs det att en "katastrof" ska hända innan någon reagerar. Tittar vi på den aktuella skandalen kring den sociala medier-jätten Facebook, som är ansvarig för data-läckaget av nästan 90 miljoner användare (Aziza, 2018), ser vi hur det är först nu som majoriteten av dess användare reagerar på deras datahantering. Som konsekvens av skandalen, börjar nu ännu fler ifrågasätta Facebook's förmåga att extrahera den här sorten av information samt argumentera för hur detta är en grov överträdelse för den personliga integriteten.

Sätter vi denna händelsen i perspektiv med om samma sak skulle ske med information som samlats in i en hemmamiljö, från det smarta hemmets enheter, kan vi snabbt föreställa oss vilken "katastrof" vi skulle stå framför. Ett läckage av denna typ av data, som utgörs av ytterst personlig och känslig information, skulle vara otroligt kritisk och kunna kränka den personliga integriteten på flera plan om vi tittar på Kommittédirektivets (2014) bestämmelser om den personliga integriteten. Att bli "bestulen" på data som kartlägger vardagliga beteendemönster, och därmed behandlar betydligt mer detaljerad och känslig information än Facebook, skulle kunna göra de användarna otroligt sårbara. I en av våra intervjuer med användarna, uttrycker IPA1 bland annat en oro kring säkerheten av den personliga integriteten, när information och data från sociala medier eventuellt kombineras med all information som samlas in från det smarta hemmets enheter. Det finns en tydlig upprördhet för den breda kartläggning som möjliggörs genom denna typ av datainsamling och kombination av personlig data där hen gör en intressant jämförelse med dagens samhälle och Orwell's "1984". Boken är en dystopisk framtidsskildring om en regering som gör allt för att kontrollera och IPA1 säger uttryckligen att "D*et var ju en utopi då men det är ju väldigt väldigt verklighet idag."*.

1. Enheternas pålitlighet

Bör användarna lita på det smarta hemmets system?

Efter att ha undersökt vårt forskningsområde, verkar en gemensam slutsats vara att så länge det finns teknik så kommer det finnas risker och brister. I en artikel talar dataentreprenören Bruno Aziza (2018) om Facebook-skandalen och förespråkar för vikten av att inte överföra data. Han skriver bland annat att användare inte bör hata molnet som lagringsplats, eftersom det inte är lagringsplatsen som är risken utan själva överföringen. Enligt honom bör fokus ligga på att få folk att minimera dess överföring av data. Detta argument kan delvis stärkas i vår forskning genom erfarenheter som en utav de tillfrågade användarna har delat med sig utav. IPA2, berättade om incidenten kring att någon okänd användares bilder hamnade i hens moln istället för det avsedda molnet. Tittar vi även på IPA3's historia, får vi det även här bevisat att det trots allt finns en sårbarhet i överföringen av information mellan enheter och övriga system.

"[...]it obviously picked up somebody else's' signal in the room or bar where I was at. So I must've picked up somebody else's information. I've no idea who it was, but it must have been someone in that same place." - IPA3, personlig kommunikation, 30 april 2018.

Genom intervjun med IPFR kan vi se hur det finns en vilja att skydda data om sina användare, där hen förklarar hur all insamlad data värderas lika högt och därmed krypteras på samma sätt. Vidare förklarar IPFR hur de lägger ner stora resurser för att kunna erbjuda produkter med hög kvalité i förhållande till dess säkerhet. Men trots företagens och tillverkarnas försök att göra överföringen säker samt IPSS's förklaring av hur överföringen oftast är säker genom krypterade strömmar, kan vi se hur det finns risker med att systemen brister och läcker känslig information om sina användare. I detta fall handlar det dock inte om risken att någon bryter sig in vid överföringen av informationen, utan teknikens bristfälligheter som genererar ofrivillig spridning av information om personlig data till externa och egentligen obehöriga parter.

Precis som samtliga intervjupersoner är överens om, och som även CIA-triaden indikerar på, bör de smarta enheterna uppnå konfidentialitet genom att exempelvis skapa behörigheter och begränsningar i systemen. Genom detta minimeras risken för att obehöriga ska komma åt en användares data. På så vis möter systemen majoriteten av de intervjuade användarnas önskan om att inte sprida de smarta enheternas insamlade data till andra system som användaren inte är helt medveten om. Tar vi Google Home som exempel gör de dock exakt det som de intervjuade användarna inte vill att de ska göra. Så fort deras användare använder sig av Googles olika

tjänster, finns en potentiell möjlighet att delar av användarens data sprids till dess vänner som kortast. Google (2018) nämner bland annat hur de kan kombinera personliga uppgifter från en tjänst med uppgifter från Googles andra tjänster. Google har påstått att syftet med denna typ av dataspridning är för att göra tjänsterna mer effektiva för användaren.

"[...]många har en känsla när du har en kamera, så ser du kameran, tänker du 'mhm vem kollar på mig nu?'" - IPFR, Personlig kommunikation, 2 maj 2018

Jämför vi sedan problematiken med Big Data dimensionen *volatility*, finns det även ett problem med real-time-data, där det är svårt att avgöra vilken data som är av relevans. Det är viktigt att identifiera ogiltig data som ligger lagrad för att kunna uppdatera med ny data (Ali-ud-din Khan, Uddin & Gupta, 2014), samt för att inte låta en obehörig person få tag på det. Volatitlity får alltså en indirekt koppling till ett systems konfidentialitet, där datans "bäst-före-datum" är viktig att bestämma för att möjliggöra en korrekt klassificering av privat data. Precis som IPFR berättar, är många användare skeptiska mot bland annat säkerhetskameror eftersom användaren känner ett obehag av att kamerorna skapar en risk för att obehöriga kan se dem i sitt hem. IPFR berättar dock att det finns säkerhetsfunktioner i kameran som de erbjuder användaren, vilket innebär att kameralinsen kan täckas för genom ett "lock". Men trots detta skydd, elimineras inte risken för att obehöriga kan få tillgång till känslig information. I förhållande till begränsningar för åtkomsten av realtidsdata och insamlad data, berättar dock IPFR hur de själva och många andra företag, ofta använder någon typ av administrationsverktyg för att begränsa möjligheten att obehöriga får tag på känslig information. Detta tyder på att vissa företag arbetar med behörigheter för att respektera användares integritet, vilket hjälper till att säkra datans konfidentialitet genom att de sätter spärrar för vem som kan och får se vad.

Som IPA3 förklarade, råkade hens enhet plocka upp någon annans styrsystem, vilket inte bör hända om det finns säkra behörigheter och begränsningar. Detta är något som tar oss till nästa problematik, där majoriteten av de tillfrågade ansåg att det fanns en viss risk att data skulle kunna bli manipulerad. Det går alltså att dra slutsatsen att användare känner en viss oro för hur trovärdiga deras system samt data är.

Ali-ud-din Khan, Uddin, & Gupta, (2014) förklarar i sin studie att det är av stor vikt att kunna särskilja vilken data som är sporadisk eller regelbunden, för att i slutändan kunna frambringa pålitliga analyser och resultat. Här kan vi se hur viktigt det är att ta hänsyn till dimensionen Volatility för att dataanalysen av de personliga uppgifter i smarta hem ska kunna generera pålitliga resultat och lämpliga funktioner åt användaren.

Detta leder till nästa utmaning som organisationer står inför, då de även måste ta i beaktning och fastställa vilket "utgångsdatum" datan ska ha. Idag, med real-time data, krävs att organisationer

ska ha förmågan att avgöra vilken data som inte längre är relevant för aktuella och nuvarande analyser som görs i *Middleware Layer*, samt hur länge all data ska lagras, vilket dimensionen *volatility* kan hjälpa organisationer att strukturera upp. Samtidigt som organisationer måste bestämma hur länge datan ska lagras, skapar det även en konflikt då organisationer samtidigt måste säkerställa att användarnas data alltid ska vara tillgänglig för dem, speciellt i akuta fall som till exempel kräver att medicinsk data måste hämtas. Att möta kundens behov är särskilt viktigt i en konkurrenskraftig bransch, där teknologin är vinstdrivande. Detta görs i *Application Layer* där det sker realisering av fullständig hantering och administrering av de praktiska tillämpningar (Khan et al. 2012), utifrån den objektspecifika information som hanteras i *Middleware Layer* som är baserad på användarnas behov.

2. Otydlig data

Varför vet inte användarna om vilken information som samlas in, hanteras och lagras?

Likt tidigare forskning visar på, bör företagens användarvillkor och säkerhetspolicyer förenklas för att göra det enkelt för användarna att förstå vad som egentligen godkänns (Struse et al. n.d.). I studien som utfördes av Struse et al. (n.d.) bevisar de hur användare ofta godkänner användarvillkor om det finns en vilja eller behov av att använda, trots att de inte förstår innebörden av vad de godkänner. Detta är någonting som tydliggörs i intervjun med IPA6, där hen berättar hur användarvillkoren ofta godkänns trots att man som användare kanske inte förstår textens verkliga mening. Betydelsen av att kunna förstå innebörden av någonting, är en aspekt som också Big Data's dimension Validity beaktar (Ali-ud-din Khan, Uddin & Gupta, 2014). Den belyser bland annat betydelsen av att data är korrekt och exakt i förhållande till det tänkta användningsområdet, vilket även framgår av Struse et al. (n.d.)'s studie där de bland annat förklarar hur en tredjedel av studiens deltagande Android-användare inte fullt kunde förstå definitionen av "Full Internet Access".

"This points to a serious security problem: if users cannot understand the permissions they grant they are likely to allow Trojan software directly through their front door by clicking at dangerous permission sets." - Struse et al. (n.d.)

Likt Struse et al. (n.d.) förklarar, är det otroligt viktigt att användarna förstår användarvillkoren, för att kunna utföra rationella beslut. Intervjuerna med användarna visade även vikten av att efterfrågad information är lätt att hitta om användarna söker den. Problematiken med att hitta rätt information i textmassan verkar vara en av de största orsakerna till att de intervjuade användarna

valde att inte läsa användarvillkoren och säkerhetspolicyer. IPA1 berättar att man som användare vet att informationen oftast finns där och att det är upp till gemene man att godkänna eller inte. Samtidigt förklarar hen att det är alldeles för mycket text att läsa igenom och att användarvillkoren oftast bara godkänns slentrianmässigt som en konsekvens av bristande ork.

"[...]man vill ju få in den nya produkten som man just har köpt, då vill man använda den med en gång. Då sitter man inte tre timmar, fyra timmar och läser igenom en jävla godkännande i någon text." - IPA1, personlig kommunikation, 29 april 2018.

Det är inte utav omöjlighet att göra det tydligare för användare vilken den exakta data som samlas in är. Detta eftersom identifiering av objektspecifik information sker i tidigt skede i processen för datainsamling hos IoT-enheter, alltså i det första lagret *Perception Layer* (Farooq et al. 2015). Därmed vet företag sedan tidigare vilken data de söker och varför, vilket därför skulle enkelt och kortfattat kunna presenteras för användarna i säkerhetspolicyer samt användarvillkoren.

Jämför vi användarnas problematik kring åtkomst av korrekt information med Big Data's dimension "volume", kan vi se tydliga samband med hur stora mängder data påverkar utfallet av informationshanteringen. På samma sätt som stora mängder data försvårar hantering av information för ett system, kan vi tänka oss hur det försvårar informationshanteringen ur ett mänskligt perspektiv. Genom sätta dimensionen i perspektiv med svaren från de intervjuade användarna, kan vi se hur stora volymer av data försvårar användarens möjlighet att hitta efterfrågad information. Eftersom flera av användarna upplevde att det krävdes en stor ansträngning för att hitta önskad information, kan vi se hur behovet av att läsa igenom hela texten bortprioriteras eftersom det tillfälliga och egentliga intresset är att använda produkten som införskaffats. Inte att skydda säkerheten av sin personliga integritet ur ett långsiktigt perspektiv. Detta bekräftades även av IPSS, att det blir för komplicerat och för mycket jobb att gå igenom säkerhetspolicyer och företagets villkor. Således kan vi bekräfta att volymen av data och information är en viktig aspekt att beakta vid utformning av användarvillkoren, där de behöver vara betydligt mindre och erhålla en tydligare struktur för att göra eftersökt information mer lättåtkomlig för användaren.

En annan orsak till varför användarna inte verkar ha tillräckligt med kunskap om vilken information som samlas in, hanteras och lagras, verkar vara den naiva inställningen till möjligheten att utsättas för de risker som finns. För vissa kan det verka obetydligt ifall viss information skulle spridas till obehöriga parter, då läckt data enbart verkar hamna och dumpas i det stora havet av övrig information. En kommentar som IPA3 nämnde var att hen ansåg sig själv vara för ointressant för att någon skulle intressera sig i att spionera på hen. Här kan vi alltså konstatera att problemet inte ligger i en icke existerande medvetenhet om integritetsrelaterade

risker hos användarna. En medvetenhet hos användarna finns, problematiken ligger snarare i det naiva förhållningssättet och inställningen "det kommer aldrig hända mig", samt att användarna ser sig själv som en i mängden. Detta är ett problem som även uppmärksammats av IPSS, där hen nämner att den naiva "det händer inte mig"-mentaliteten verkar vara en av de främsta faktorerna till att identitetsstölder uppstår idag.

"Man förstår inte den risken och hur lätt det är att ta det av information som folk bara släpper ifrån sig." - IPSS, personlig kommunikation, 2 maj 2018.

Precis som Bugeja, Jacobsson och Davidsson (2016) antyder om vikten av användarnas riskmedvetenhet vid användandet av smarta enheter, ser vi även hur IPSS belyser vikten av att användare förstår existensen av potentiella och säkerhetsrelaterade risker. Ett vanligt beteende som uppmärksammats av IPSS, vilket även kan kopplas till den naiva inställningen hos det smarta hemmets användare, är att användare av olika system och applikationer ofta är relativt ovarsamma med sina lösenord och information kring dem. Trots att användare är medvetna om risker, existerar det en nonchalant attityd gentemot vikten av en säker lösenordshantering. Likt det som IPSS förklarar, kan en orsak till detta naiva och ovarsamma förhållningssätt vara att användarna inte inser omfattningen av de konsekvenser som kan uppstå. Tittar vi på det smarta hemmet kan vi dock se hur lösenordshanteringen i slutändan spelar en viktig roll gentemot de intervjuade användarnas uppfattning kring ett säkert hem. Detta eftersom 83% av de tillfrågade nämnde att en av de största säkerhetsrelaterade riskerna, i förhållande till deras personliga integritet i hemmet, var att någon skulle hacka sig in på deras nätverk och få åtkomst till informationen som finns tillgänglig i de smarta enheterna.

3. Företagens datahantering

Kan användarna lita på företagen? Vem vinner mest på de smarta enheternas informationshantering?

Huruvida insamlad data är något som dessutom sprids mellan de olika tillverkarna av de smarta enheterna och deras samarbetspartners är dock relativt oklart i många fall. Tittar vi på Apple's säkerhetspolicy skriver de bland annat hur användarnas personuppgifter "[...]will not be shared with third parties for their marketing purposes." (Apple, 2018). Däremot är det svårt att hitta om personuppgifter delas med tredjepartstjänster av andra anledningar. Detta hasarderar den personliga integriteten eftersom det inte tydliggörs för användarna vem som äger rätten till den typen av data, något som även påverkar konfidentialitetsaspekten då användaren inte längre kan vara övertygad om ifall målet med att hålla datan privat och i säkerhet kan uppnås.

"689 million people across 21 countries were the victims of cybercrime last year. Is your smart home leaving the door open?", Norton (2018).

Efter att IPSS förklarat att det är sällan företag anmäler sina intrång eftersom det är dålig reklam för dem, går det att undra om en användare verkligen kan lita på vad företag väljer att säga utåt och vad de väljer att dölja. Vilket verkar också vara ett bekymmer bland de intervjuade användarna, då IP6 bland annat uttrycker sig med *"[...] i deras mörkaste rum [...]*" och IP5 säger att *"För det första så är det ju företags syfte att tjäna pengar. Och då överskuggar det allt annat."*, när frågor har ställts om hur företag hanterar data och risker kring den personliga integriteten. Skulle användarens data dessutom hamna i fel händer, förklarar IPSS att en konsekvens skulle vara att användare löper risk att utsättas för kriminalitet. I kommittédirektivet från justitiedepartementet (Dir 2014:65) förklaras bland annat hur personuppgifter som publiceras online löper en risk till att användas i bedrägligt syfte. Läckage av data som berör personuppgifter, men även beteendemönster, skulle kunna leda till exempelvis identitetsstöld och utpressning. Detta är exempel på två typer av brottslighet som kan tänkas öka av ett sådant läckage. Exempelvis skulle analyserad och sammanlänkad data kunna användas för att få den drabbade att utföra en handling genom hot om exempelvis skandalisering. En annan typ av utpressning skulle kunna vara att obehörig part stryper åtkomsten av hälsokritisk information för den drabbade, tills det att en lösensumma erläggs. Sätter vi ett dataläckage som detta mot CIA-triaden, ser vi hur det skulle strida mot tillgänglighetsaspekten av datahanteringens ramverk - CIA-triad - eftersom kravet om att användaren ska få kunna snabb tillgång till nödvändig och efterfrågad data (Friedman & Singer, 2014) inte längre kan uppnås.

Det är också viktigt för organisationer att bestämma hur länge data ska lagras, just för att inte obehöriga ska kunna hämta ogiltig data och eventuellt manipulera den. Samtidigt skapar detta en konflikt för organisationer då de måste säkerställa att användarens data alltid ska vara tillgänglig för dem när användaren behöver den, exempelvis i akuta fall som kräver att historisk data måste hämtas. Använder vi kameraövervakning som exempel, så spelar den in data varje sekund och samlar därför på sig en hel mängd data. Här måste organisationen väga för- och nackdelar med att lagra all den data mot varandra, samt hitta ett datum där den data överskrids eller tas bort för att skapa plats åt ny data. Samtidigt som organisationen måste ta detta beslut är det också viktigt att ha i åtanke att den data som har blivit borttagen av den enkla anledning att den är "gammal", kan behövas i framtiden till exempel om en obehörig person skulle befinna sig på användarens tomt och utan att användaren har vetat detta i flera månader upptäcks detta av ett plötsligt behov och kan därför behövas vid det fallet. Skulle den data däremot ha blivit borttagen, kan viktig data som skulle ha gett betydelse i en annan kontext ha gått miste om.

Vi kan från resultaten dra slutsatsen att de tillfrågade trodde att företagen använde den insamlade data främst till företagets syfte och inte användarnas. Men att möta kundens behov är synnerligen viktigt i en konkurrenskraftig bransch där teknologin är vinstdrivande och därför sätts organisationerna på prov när de ska utveckla IoT-enheter. Det är på så vis betydelsefullt att uppnå den funktionalitet som är tänkt för de olika lagren i IoT-enheter som Khan et al. (2012) har i sin forskning kunnat konstatera är ständigt förekommande. Vilket kan anses vara svårt efter att hackare ändå har lyckats komma åt data eller som IPA3 lyckats göra, att ta över någon annans styrsystem.

Jämför vi användarnas problematik med Big Data dimensionen *veracity*, går det att förstå att oron kommer ifrån all den data som ständigt skapas och att det blir därmed svårare att hantera samt kontrollera det. Vilket därför skapar en utmaning för organisationer, där de ständigt måste kritiskt granska den insamlade data.

4. Datas förmåga att påverka

Varför anser användarna att datainsamlingen anspelar på deras personliga integritet?

En nyhet som nämndes under intervjuerna av användarna, var den stora och väldigt aktuella skandalen kring den sociala medie-jätten Facebook, som är ansvarig för data-läckaget av nästan 90 miljoner användare (Aziza, 2018). Efter att ha studerat de intervjuade användarnas svar på frågor om vilka risker de ser med det smarta hemmets datainsamling och hantering, verkar exponering av krisrelaterade nyheter vara en orsak till att individer skapar sig en alltmer kritisk bild av dagens teknik. En konsekvens av att exponeras för stora "katastrofer" som Facebook-skandalen, verkar vara att de smarta hemmets användare får en ökad medvetenhet kring potentiella risker som kan uppkomma från den datainsamling som sker av de smarta enheterna.

Efter att ha studerat resultaten har vi även kunnat konstatera att en del av de säkerhetsrelaterade riskerna gentemot den personliga integriteten, verkar ligga i att betydligt mer data än nödvändigt samlas in från tillverkarna av smarta enheter (Molina-Markham et al. 2010). De nämner även den stora simpliciteten för dem att samla in personligt identifierbar data genom enbart smarta termostater, och sätter möjligheten för denna datainsamling i perspektiv till enheter som har tillgång till tusentals hem. Det är viktigt att förstå förmågan hos data för att se dess värde och möjligheter, men även för att förstå de risker som kan identifieras med den. Hur något som till en

början kan vara flera till varandra oberoende komponenter, kan sedan sammankopplas och analyseras.

Genom att undersöka dimensionen *variety* i ramverket för Big Data, går det att konstatera att det finns en viktigt betydelse av att koppla ihop rätt data till rätt användningsområde för att kunna utvinna värdet i den specifika data (Perwej, 2017) . Dessutom går det även att hitta ett samband med dimensionen *valence* som visar på att det går att hitta direkta eller indirekta kopplingar mellan olika komponenter genom att mäta och undersöka den insamlade data (Atanassov et al. 2016). Hittar vi kopplingar mellan olika komponenter ser vi hur integriteten med systemet kan uppnås och användaren kan därmed ha förtroende till att systemet de använder sig utav beter sig på det sätt som är förväntat och att de får resultat som är trovärdiga.

För att lösa problemet med att datainsamlingen anspelar på den personliga integriteten och låta en användare vara anonym, skulle företag kunna ta efter IPFR sätt att ansluta en ny användare till deras system, där användaren endast behöver ange mailadress och lösenord för att aktivera sitt konto. På detta sätt skulle det kunna bli möjligt för företagen att fortsätta föra statistik och utföra marknadsanalyser, utan att användarna behöver kunna identifieras och därmed undvika viss risk för intrång av deras personliga integritet.

5. Rädsla kontra fördelar

Finns det säkerhetsrelaterade risker som kan genereras med eller ur känslig data? Och varför fortsätter användarna att använda sig av de smarta enheterna, fastän de är medvetna om systemens brister?

När de smarta hemmets användare intervjuades, framkom det tydligt att samtliga värdesatte rätten till privatliv. När vi bad de intervjuade användarna att förklara sin definition av personlig integritet, nämnde 100% av de tillfrågade att benämningen handlade om möjligheten att vara privat. IPA6 förklarade bland annat hur det inte gjorde så mycket om en bild lades ut på hen i ett forum, där ingen vet vem hen är eftersom att inga personliga uppgifter var kopplade till hen. Vidare menar dock IPA6 att så fort bilden kunde kopplas till hen som individ, genom exempelvis namn och adress, skulle åsikten ändras och dataanvändningen inte uppfattas som acceptabel.

”[...]det är i alla fall inte den här systematiska insamlingen av information.” - Personlig kommunikation, IPA4, 1 maj 2018.

Efter att ha jämfört de empiriska resultaten med varandra, kan vi avläsa att de smarta enheternas användare som intervjuades, uppfattar en nervositet över deras oförmåga att kontrollera och hantera spridningen av data om dem. IPA4 berättar bland annat hur hen avstår från användandet av vissa smarta enheter och sociala medier, som en konsekvens av den systematiska insamlingen av informationen som sker av dessa system. Här kan vi se hur Big Data-dimensionen Velocity påverkar användarnas uppfattning om de smarta enheternas informationshantering i en negativ tappning. Försöker vi sätta dimensionen i perspektiv till det smarta hemmet, ser vi relativt snabbt hur det är en ytterst viktig aspekt i förhållande till om spridning av data är kontrollerbar eller inte. Om data samlas in från de smarta hemmet, kan den analyseras och därmed generera ny och ökad mängd information. Senare kan detta leda till att användarens vanor kartläggs, vilket genererar ännu mer ny och ökad mängd information. Risken innebär alltså främst att de smarta enheterna gör det möjligt att en för användarna omedveten spridning av information kan ske.

Som IPFR och IPSS indikerar, ligger en del av ansvaret på att användaren måste läsa igenom användarvillkoren för att förstå vad som sker med deras data. Detta är viktigt för att användaren inte ska godkänna företagens rättigheter att vidta åtgärder som konsumenten inte känner till eller är bekväm med. Dock finns det idag inga möjligheter för en konsument att bestämma och ändra avtalet och måste därför godkänna villkoren för att kunna börja använda sin produkt.

Det är genom data analytics som det smarta hemmet besitter förmågan att kunna analysera dataströmmar, och därmed skapa ett verkligt värde av såväl rådata som information (Leuschner, 2017), vilket är i lagret *Business Layer* där data omvandlas till ett värde och därmed vinstdrivande Khan et al. (2012). Tittar vi även på IPA1's oro om möjligheten att kombinera det smarta hemmets insamlade data och den individrelaterade data som systematiskt samlats in från exempelvis sociala medier, kan vi tänka oss hur accelerationen för alstrandet av ny data kan öka drastiskt.

> *"[...]hur kan man bygga ihop allting så att det kopplas till mig?"* - IPSS, Personlig kommunikation, 2 maj 2018.

I intervjun med IPSS, var det en del ur hens definition av personlig integritet som särskilt berörde problemet kring datans transmigration. Hen förklarar hur personlig integritet handlar om vilka som får tillgång till data om enskilda individer samt hur datan som individen lämnar ifrån sig kan byggas ihop och kopplas tillbaka till den enskilde. I förhållande till säkerheten av den personliga integriteten, ser vi även hur kommittédirektivet från justitiedepartementet (Dir 2014:65) talar om vikten av individens rätt att kunna kontrollera vem som får tillgång till känslig information om den enskilde. Genom samtliga intervjuer med användarna, kan vi se hur ofrivillig spridning av känslig information och kartläggning av individen är två scenarion som samtliga användare upplever som ytterst kritisk i förhållande till att det smarta hemmet ska

kännas pålitligt. Här verkar en av orsakerna till detta ställningstagande vara individens känsla av den maktlöshet som IPA2 talar om i sin intervju, där hen bland annat förklarar sin oförmåga att veta om data manipuleras eller inte eftersom hen inte ens har möjlighet att veta vem som har tillgång till den. IPSS framhäver i sin intervju att tillgång till någons inloggning, banker eller personlig information är lika känsligt eftersom det fort går att kartlägga information om individen och på så vis kan den obehöriga utnyttja situationen till sin egna vinning.

En säkerhetsrelaterad risk som nämndes i intervjuerna med användarna, var eventualiteten att obehörig part får åtkomst till personlig data genom att hacka sig in på nätverket och i enheterna. Skulle detta ske, betyder det att konfidentialitetsaspekten av datahanteringens ramverk - CIA-triad - bestrids eftersom obehöriga parter riskerar att få tillgång till personuppgifter och känslig data. En av de främsta orsakerna till att 57% av de intervjuade användarna anser kategorin säkerhet som en av de känsligaste områdena i förhållandet till deras personliga integritet i hemmet, verkar grunda sig i den tydliga kopplingen till uppenbara brott såsom inbrott och stöld av pengar. Samt att det går att utvinna väldigt känslig information om användaren, som den smarta enheten kan ha samlat in.

"[...] kan jag då sitta på andra sidan jorden och låsa upp dörren så kan någon annan sitta och låsa upp dörren utan att jag vill det så att säga." - Personlig kommunikation, IPA2, 29 april 2018.

Tanken på att obehöriga parter skulle hacka sig in på enheter som hanterar data med en så tydlig koppling till säkerhet av deras personliga integritet, verkade skrämma användaren mer än risken för läckage av data som exempelvis möjliggjorde kartläggning av deras favoritfilmer.

Ytterligare data som vi kunnat konstatera är en av de mest kritiska i förhållande till säkerhet av den personliga integriteten, är data med en hälsomässig koppling. Detta är även någonting som upplevdes av de intervjuade användarna, där 29% av de tillfrågade bedömde att hälsorelaterad data kunde utsätta säkerheten av den personliga integriteten i det egna hemmet för risk och skada användaren såväl fysiskt som psykiskt. IPA1 berättande bland annat om ett orosmoment inför framtiden, med en möjlig konsekvens av att information som innehåller individens sjukdomstillstånd blottas. Hen förklarar risken med ökade samhällsklyftor, vilket skulle kunna bli en konsekvens om försäkringsbolag kan köpa hälsorelaterad information. Genom uppköp av data med en hälsomässig koppling, kan försäkringsbolagen få tillräckligt med kunskap om individers sjukdomstillstånd och använda det i bedömningen om en individ är berättigad sjukförsäkring eller inte. Ett resultat av detta skulle kunna vara att folk nekas ta försäkringar på grund av att de är sjuka alldeles för ofta och enbart accepteras för folk som helt friska. I slutändan riskerar vissa människor att bli helt utan försäkringsskydd, vilket i sin tur riskerar en ökad divergens i samhället.

Ett annat scenario som uppkom i intervjuerna av det smarta hemmets användare, var den potentiella möjligheten för individualiserad marknadsföring som spelar på användarens emotionella tillstånd. Om hälsorelaterad data om individer samlas in från enheter i hemmet och analyseras av verksamheter, kan kartläggning ske av vardagliga vanor och personliga beteendemönster ske. Orsaken till att detta ansågs inkräkta på den personliga integriteten verkar ligga i verksamhetens möjlighet att utnyttja individens mentala tillstånd för att sälja mer genom det som IPA7 förklarade som en skrämselteknik. Exempelvis att om de smarta enheterna registrerar att användaren hyser en rädsla för skadedjur, finns möjligheten att verksamheterna antyder på ökad förekomst av skadedjur i sina kampanjer, med mål om att skrämma användaren för att kunna sälja fler produkter. Risken här är alltså att möjligheten att någon, företag eller obehöriga parter såsom hackare, ska utnyttja användares emotionella tillstånd för egen vinning. För

Med hälsorelaterad data kan vi alltså se hur den, ensam och i kombination med annan data, kan utgöra en risk för individens säkerhet ur ett långsiktigt perspektiv. Eftersom risken finns att exempelvis hälsorelaterad data utnyttjas av obehöriga parter och används åt fel syfte, inkräktar på det CIA-triaden integritetsaspekt (Evans, Bond & Bement, 2004). Likt Metivier (2017) förklarar, är det viktigt att användaren kan lita på att systemet följer “code of ethics”, för att de smarta enheterna ska kännas pålitligt. Enligt de intervjuade användarnas uppfattning är betydelsen av att data hålls konfidentiell ytterst viktig, för att inte äventyra säkerheten av dataintegriteten samt den personliga integriteten i hemmet.

Efter att ha analyserat svaren från de intervjuade användarna, verkar som att deras svar går hand i hand med lagstiftningen om hur känsliga uppgifter bör behandlas genom ett starkare skydd i GDPR (Datainspektionen, 2012). De intervjuade användarna ansåg bland annat att det bör finnas en möjlighet till att själva få bestämma vad deras data ska användas till samt godkänna vilka mottagare som ska få tillgång till deras data.

Trots de medvetna riskerna använder de intervjuade användarna sina smarta enheter i hemmet, vilket kan tyckas vara lite underligt utifrån det som sagts i intervjuerna gällande detta. När vi frågade varför de ändå väljer att använda sig utav de smarta enheterna, var svaren rätt så splittrade och kunde delas in två grupper. Den ena ansåg att vinsten är större än risker, medan den andra ansåg att de blir tvingade till att använda sig utav det som en följd av samhällets utveckling, som resulterar i att det är svårt att ta sig ur användandet av smarta enheter i hemmet. För den skara som ansåg att vinsten vad större än risken, förklarade bland annat IPA3 hur hen ansåg att information och data om hen skulle delas, oavsett om hen fortsatte använda sig av smarta enheter i hemmet eller inte. Därför ansåg IP3 inte att de smarta enheterna utgjorde en större risk än någon annan teknisk enhet som hanterar personlig information.

"Nej det finns inga dumma TV:s längre haha." - Personlig kommunikation, IPA4, 1 maj 2018.

I den skara som istället ansåg att de blev delvis tvingade in i användandet av smarta enheter, berättade IPA4 bland annat hur hens användande av exempelvis en smart-TV, är ett resultat från avsaknaden av valmöjligheter för huruvida individen själv kan välja att använda vissa smarta enheter i vardagen eller inte. Om vi tittar på detta scenario där användarna känner sig påtvingade att använda smarta enheter eller att de nödvändigtvis behöver använda den, ska de inte kunna ha något inflytande eller ställa krav på hur deras datahantering sker efter att de har börjat använda sig utav produkten? Eller ska de bara acceptera att deras personliga information används och delas lite hur som helst av de smarta enheterna och gilla läget utan att faktiskt veta vad som händer med den? Enligt datainspektionen (2012) bör svaren till dessa frågor vara glasklart. Den personliga integriteten måste skyddas och sättas i första hand.

"Några grundläggande principer inom integritetsskydd är att inte samla in mer information än vad som behövs, inte ha den kvar längre än man behöver och inte använda den till något annat än vad man samlade in den för. Att informera om hur uppgifterna ska behandlas, att begära samtycke och att tillåta insyn i den vidare hanteringen är också led i integritetsskyddet." - Datainspektionen (2012).

Datainspektionen (2012) påpekar tydligt att det är användaren som ska ha rätten till att bestämma hur deras egna data ska behandlas och hanteras, vilket även de intervjuade användarna ansåg ha rätten till. Det är alltså inte så svart på vitt som många tycks tro, utan det är något som är fullt möjligt att uppnå, om bara organisationerna följer detta ramverk och regler för att tillåta användaren att få kontroll över hur deras data behandlas och hanteras. I ett tidigt skede av utformning av system bör kriterierna för den personliga integriteten tas i beaktning för att det inte ska bli för komplicerat och därmed dyrt att åtgärda (Datainspektionen, 2012). Dessutom för att användaren ska kunna lita på datainsamlingen, hanteringen och lagring bör alltså organisationer vara transparenta med hur de hanterar och behandlar sina konsumenters data. Det intervjuade företaget hade kommit en bra bit på vägen till att vara helt transparenta genom att logga enheternas aktivitet i huben, för att låta användaren ta del av systemets processer. Dock skulle det optimala vara om de även hade loggat användningen utav användarens data. Där användaren kan få se vart deras data används och på så vis få en direkt återkoppling som skapar transparens. Dessutom bör IT-systemen vara utformade på det sätt att de endast samlar in och hanterar de personuppgifter som krävs för funktionerna och för att uppfylla ändamålet, vilket de intervjuade användare och Datainspektionen (2012) belyser som en viktig del av den personliga integriteten.

Som tidigare nämnts och som IPSS förklarade under sin intervju, är det viktigt med behörigheter i system för att anställda ska få tillgång till icke-relaterade data till deras arbetsuppgifter, vilket på det sättet skulle kunna bidra med en ökad pålitlighet från konsumentens perspektiv. Det skulle kunna visa för konsumenten att företaget tar den personliga integritet på stort allvar.

För att skydda den personliga integriteten föreslår Datainspektionen (2012) bland annat att ersätta namn med till exempel pseudonymer, vilket skulle tillåta användarna vara anonyma. IPFR skyddar sina användares personliga integritet där de bland annat tillåter användarna att vara anonyma när de ansluter sig till tjänsten. De ber endast sina användare om mailadress och lösenord när de skapar ett konto för deras system. På så vis kopplas inte data så att det riskerar att inskränka på den personliga integriteten, lika tydligt som om det vore krav på att ange kön eller personnummer.

6. Slutsats

I detta avsnitt presenterar vi ett lösningsförslag utifrån det vi kommit fram till i uppsatsens diskussionsdel. Slutligen presenteras även förslag för eventuell vidareforskning av vårt forskningsområde.

6.1 Lösningsförslag

Forskningsfrågan som ställdes i början av denna uppsatsen var:

Ur ett användarperspektiv - Vad indikerar pålitlighet inom ett smart hem där data delas per automatik via smarta enheter?

Efter att ha kritiskt granskat såväl empiriskt som teoretiskt insamlat material, har vi genom resultaten kunnat fastställa att det främst är fyra faktorer som indikerar pålitlighet inom ett smart hem ur användarens perspektiv. Dessa har vi sammanställt genom en akronym vi valt att kalla MITT - *Medgivande*, *Inflytande*, *Tydlighet & Tillgänglighet*.

Medgivande
Denna faktor behandlar företagens skyldigheter i förhållande till säkerhet av personuppgifter. En konsument ska även kunna ha möjligheten till att få bestämma om hen vill vara anonym eller inte vid användningen av den smarta enheten. Detta skulle kunna ske genom att ersätta namn med till exempel pseudonymer. Eftersom problematiken att individer inte vill att deras data ska samlas in för något annat syfte än för huvuduppgifterna, grundas i, enligt våra resultat, att datainsamlingen inte bör inskränka på deras personliga integritet. Vilket skulle kunna medföra att organisationer kan fortsätta samla in data till reklam eller liknande om konsumenten får lov att vara anonym i det hela. IT-system ska helst vara utformade så att så få personuppgifter som möjligt samlas in och hanteras. Det behöver fastställas vilka personuppgifter som verkligen krävs för att tillgodose ändamålet, snarare än att se vilken data som finns tillgänglig att samla.

Inflytande
Under samtliga intervjuer med det smarta hemmets användare, framkom åsikter om att samtliga önskade att de kunde ha ett större inflytande av de smarta enheternas datahantering. För att skydda den personliga integriteten är det viktigt att begränsa datainsamlingen genom olika tillvägagångssätt, där användaren själv kan bestämma vilken data som får samlas in, spridas och delas med andra parter. Dessutom bör en användare kunna vid behov ha möjlighet till att ta bort all data som är kopplat till hen. Andra metoder som att begränsa datainsamlingen genom att endast hantera uppgifter som indirekt pekar ut en individ skulle kunna användas. Det avser att till

exempel personnummer inte ska vara en nyckel i databaser. Användare ska alltså inte behöva känna att de måste acceptera alla användarvillkor och säkerhetspolicy utan att ha något inflytande på vad de faktiskt vill acceptera.

Tydlighet

När vi sedan går in på huruvida användarvillkor utformas och dylikt, är det viktigt att de håller en simpel struktur som är lättläst för samtliga individer, oavsett vilken teknisk kunskap de besitter. Här är det viktigt att företagen visar vad som händer med den data som samlas in genom att göra en tydlig kartläggning av datahanteringen för användarna. Här bör frågor som "Vem äger datan?" och "Vad används datan till?" framgå tydligt. Hela 64% av de tillfrågade användarna svarade att de långa och otydliga användarvillkoren resulterat i att de inte orkat söka efter vilken information som samlades in om dem. Användarna nämnde även vikten av att informationen presenteras på ett användarvänligt och simpelt sätt.

Här skulle ett lösningsförslag kunna vara att införa en global standardisering av symboler för vilken och hur information hanteras. Likt IPA7 nämner är det så det funkar i trafiken, att trafikregler är exponerade genom trafikskyltar för att trafikanterna snabbt och enkelt ska kunna förstå vad som gäller. På samma sätt skulle detta kunna appliceras för användarvillkoren, där symboler ger användaren en snabb överblick av de smarta enheternas sätt att informationshantering.

Tillgänglighet

För de intervjuade användarna visade det sig även att tillgängligheten av information var viktigt. Med detta menar vi att det ska vara lätt för användarna att hitta informationen om datahantering. Att det ska vara lätt att hitta korrekt information om en användare försöker söka efter någonting. För att användare lätt ska kunna förstå och hitta information, är det viktigt att information om samma sak inte är utspridd på olika sidor utan är placerad på ett och samma ställe.

I MITT innefattar *tillgänglighet* även möjligheten att användare ska lätt kunna hitta funktionerna där de hanterar inställningar för vilken data som samlas in och liknande. För att lösa problematiken som användarna upplevde kring ofrivillig spridning av information, skulle ett lösningsförslag kunna vara att, så fort någon använder en användares data, ska detta loggas. Detta innebär att en användare ska kunna se all historik för all informationsanvändning. Företaget bör därför utgå från en transparent modell, som kan göra det enkelt för användaren att följa upp deras datahantering, samtidigt som känslig data om den enskilde inte riskerar att spridas till obehöriga parter.

MITT

För att komma fram till MITT, har vi bland annat satt samtliga resultat i förhållande till Big Data's dimensioner. Orsaken till att vi ser dessa dimensioner som lämpliga att arbeta med, i vår studie för vad som indikerar pålitlighet i det smarta hemmet, är att dimensionerna hjälper oss att förstå hur de smarta enheterna bör behandla information för att indikera pålitlighet för användarna. Vi har även arbetat med att titta på såväl det teoretiska som det empiriska materialet med hjälp av CIA-triaden, vilken har underlättat och ökat vår förståelse kring vad som bör tas i beaktning vid hanterandet av känslig data. Tillsammans anser vi att dessa två redan beprövade och välanvända teoretiska delar, har hjälpt oss vid utvärdering och framtagandet av trovärdiga slutsatser och resultat.

Eftersom det även finns påvisad statistik för att marknaden för smarta hem genomgår en drastisk expansion (Statista, 2018), finns eventualitet att datainsamling från det smarta hemmet bidrar till expansionen av big data i framtiden. Genom att därmed använda sig av big data's dimensioner i framtagningen av MITT, förbereds datahanteringen för det smarta hemmets enheter inför framtiden.

6.2 Förslag till vidareforskning

För vidare forskning vore det intressant att göra en kvalitativ eller kvantitativ forskning ur ett tekniskt perspektiv. Nästa steg skulle kunna vara att skapa tekniska mål med MITT som grund. Eftersom vår studie omfattar endast hur pålitligheten för de smarta enheterna ska förstärkas ur ett användarperspektiv, skulle det vara intressant om framtida studier även undersöker vilka funktioner i de smarta enheterna som skulle kunna förstärka denna pålitligheten. Exempelvis skulle det vara av intressant att undersöka GDPR's krav på hur dataminimering ska hanteras ur ett tekniskt perspektiv, för att se hur de funktionella delarna bör lösas.

7. Bilagor

7.1 Intervjuguider

7.1.1 Bilaga 1 - Användare

MODELL	**FRÅGA**
Bakgrund	● Vad är er definition av personlig integritet?
IoT	
Perception Layer	● Har du tittat upp vilken information som de smarta enheterna samlar från dig? Om JA: ○ Var det lätt att hitta informationen? ○ Har du försökt ta reda på det? ○ Anser du att informationen som fanns tillgänglig, för vilken data som samlas in, var tillräcklig? Varför/Varför inte? ● Hur ställer du dig till att de smarta enheterna samlar in data om dig?
Network Layer	● Hur ser du på kommunikationen som sker mellan enheterna? Pålitlig/Riskfylld? ● Litar du på att den insamlade datan överförs på ett säkert sätt mellan de smarta enheterna du använder och övriga system som hanterar dess data (exempelvis företagens servrar)? Varför / Varför inte?
Middleware Layer	● Vet du hur den insamlade datan hanteras av företagen? Dvs, vad som händer med datan efter att den samlats in av företagen? Om JA: ○ Var det lätt att hitta informationen? Om NEJ: ○ Finns det någon orsak till varför du inte tagit reda på det? ○ Har du försökt ta reda på det? ● Vad är din åsikt om företagets/företagens sätt att hantera den data de samlar in från dig genom de smarta enheterna? Om JA: ○ Hur ställer du dig till det? ○ Vet du vilka som har tillgång till den insamlade datan?

Application Layer	• Vilken är den främsta orsaken till att du införskaffade dig smarta enheter?
Business Layer	• Tror du företagen försöker vara tydliga kring vilken data som samlas in och hanteras? Varför/Varför inte? • Tror du att företag använder den data som samlas in från ditt hushåll, främst för sitt eget syfte eller för dig som användare?
CIA-triad	• Ser du några risker för hushållets personliga integritet vid användning av smarta enheter? Om JA: o Påverkar dessa risker valet av vilka smarta enheter ni använder er av? o Använder ni smarta enheter, trots riskerna, på grund av att ni anser att ”vinsten” är större än riskerna? • Vilket område för insamlade data, anser du är mest känsligt i förhållande till den personliga integriteten? Underhållning, Hälsa, Säkerhet eller Energi? Varför? Långsiktigt/Kortsiktigt?
Konfidentalitet	• Anser du att enheterna har tillräckligt med begränsningar för olika behörigheter?
Integritet	• Litar du på att enheternas system fungerar som de ska? • Anser du att det finns risker med att din data kan bli manipulerad? Om JA: o Ser du det som ett problem?
Tillgänglighet	• Anser du att din data är alltid tillgänglig för dig när du behöver den?

7.1.2 Bilaga 2 - Företag

MODELL	**FRÅGA**
Bakgrund	● Vilka smarta hemmets produkter / enheter har ni?
IoT	
Perception Layer	● Hur samlar dessa enheter in datan? (via sensorer etc) ● Vilken data samlas in? ○ Kan ni ge exempel för de ovanstående produkter som har nämnts
Network Layer	● Vart skickas den insamlade datan sedan? (Ex svar: The cloud) Om svaret är The Cloud: ○ Har du koll på ifall molnleverantören får ta del av data eller är den krypterad? ● Hur kommunicerar enheterna med varandra? ● Får fler enheter som är uppkopplade till samma nätverk molntjänst tillgång till samma insamlad data? OM JA: ● Varför och hur långt kan detta sträckas till / vilken är avgränsningen? (Ex svar: alla enheter som är i hemmet, eller för begränsade områden, alltså för de enheter som utför samma tjänster samt behöver kommunicera för att utföra en tjänst, eller finns det ingen gräns?) OM NEJ: ○ Hur säkerställer ni att de inte gör det / vilken behörighet eller gräns finns det? ● Får en tredje part tillgång till denna data? ○ Varför? Varför inte? ● Hur säkerställer ni att datan är ”i goda händer”? ● Vilka kriterier måste denna tredje parten uppnå för att få tillgång till datan? ● Har ni någon slags verifiering för detta?

Middleware Layer	● Vad händer sedan med den insamlade data? ● Hur länkar ni samman system för att utföra handlingar och beslut för att garantera samma servicetyp mellan de anslutna enheter. ● Vad gör systemet sedan med denna information?
Application Layer	● Hur möter man kundernas behov? ● Vart ligger fokuset på affärsidéerna, är det för att underlätta kundens vardag, fokus på säkerhet etc.
Business Layer	● Vad är det som är vinstdrivande i smarta hem (är det datan som är vinstdrivande)? ● Hur värdefull är datan som behandlas? ● Används datan till att förutspå trender etc?
CIA-triad	
Konfidentalitet	● Vem har tillgång till systemen där datan hanteras? ● Är det några andra än ni (företaget) som har tillgång till data? ● Vilka kriterier måste uppfyllas för att få tillgång till olika behörigheter? ● Ur ett säkerhetsperspektiv, behandlas all data lika? Finns det olika nivåer för säkerheten (Tex personnummer vs. data om temperatur)?
Integritet	● Hur säkerställer man att datan i systemet är pålitlig och inte manipulerad? ○ T.ex. att medicinsk data inte ändras på något sätt utan att den som äger datan gör det själv.
Tillgänglighet	● Hur garanterar man att datan alltid är tillgänglig för användarna när de behöver den? ○ T.ex. vid akuta fall, där man behöver få tag på medicinsk data?

7.1.3 Bilaga 3 - Svenska Säkerhetsmyndigheten

MODELL	**FRÅGA**
Bakgrund	● Skulle du snabbt kunna berätta om din yrkesroll? ● Vad är er definition av personlig integritet? ● Vad ser ni som den största orsaken till identitetsstölder? Finns det något mönster?
IoT	
Perception Layer	● Vilka enheter i smarta hemmet kan vara mest utsatt för externa attacker? ● Hur kan man som användare förhindra att känslig information kommer i fel händer? ● Brukar mer data än nödvändigt samlas in om användaren från företag? ○ Varför / Varför inte?
Network Layer	● Vad finns det för risker med att personlig data överförs mellan enheter? ○ Hur kan det påverka individens personliga integritet? ● Vid intrång på nätverket, hur lång tid brukar det ta innan man upptäcker det? ○ Individnivå vs. organisatorisk?
Middleware Layer	● Vid intrång där data lagras, hur lång tid brukar det ta innan man upptäcker det? ○ Individnivå vs. organisatorisk?
Application Layer	● När man realiserar smarta enheter/enheter som samlar in och administrerar data, vart bör fokus ligga (Säkerhet vs. Effektivisering)?
Business Layer	● Gör företagen tillräckligt för att tydliggöra för individen vad för data som behandlas? Varför / Varför inte? ● Gör företagen tillräckligt för att tydliggöra för individen för vilka säkerhetsrisker som kan uppkomma vid användning utav deras tjänster? Varför / Varför inte?
CIA-triad	
Konfidentalitet	● Är behörigheter viktiga ur ett företagsperspektiv och kundperspektiv? ○ Varför / Varför inte? ● Hur bör man kontrollera behörigheter? Stämmer det överens om hur de oftast kontrolleras idag? ● Hur kan man som användare förhindra att känslig information om en själv hamnar i fel händer?
Integritet	● Vilken data samlas in som ni anser kan vara mest känslig? ● Tror du GDPR kommer hjälpa till i skyddandet av den personliga integriteten, ur användarens perspektiv? ● Vem äger rätten till den data som samlats in av företagen?
Tillgänglighet	● Är tillgänglighet av data viktig för privatpersoner? ○ Varför? / Varför inte?

7.2 Transkribering av intervjuer

7.2.1 - Användare 1 (IPA1)

Datum: 2018-04-29, 21:14-21:43
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Och då vill jag bara börja med att fråga dig vad är din definition egentligen av personlig integritet?

(U)
Oj haha. Jaha, personlig integritet för mig är att uppgifterna kring mig och min person är skyddade mot andra personer om jag inte ger tillstånd till det. Det kan man väl säga att det är min definition på personlig integritet.

(I)
Mm, perfekt tack. Och om vi då tänker på kring det smarta hemmet, som du använder dig av. Hur ställer du dig till att de smarta enheterna samlar in data om dig [...]?

(U)
Ja det beror ju på vad informationen används till. En sak är ju om jag kommer hem, jag personligen, och jag vill ha, normalt så brukar jag vilja ha en viss temperatur, och att den då hör att det är jag och ställer in den temperaturen, då är det ju bra så att säga. Men sen är det ju då om den som äger programvaran samlar in information och säljer eller sprider vidare den informationen som smarta hemmet samlar in. Det är väl det som är, ja risken eller det som är otrevligt eller för att man kan kartlägga personer väldigt in i minsta detalj utan att man tänker på det eller vet om det.

(I)

Mm. Har du tittat upp vilken information som de smarta enheterna, som du använder dig av, samlar in från dig?

(U)
Nej. Det har jag inte gjort.

(I)
Finns det någon orsak till att du valt att inte ta reda på det? Till varför du inte har gjort det?

(U)
Slöhet haha.

(I)
Haha okej. Så du har då alltså inte försökt ens att ta reda på vilken information som tas upp från dem?

(U)
Nej det har jag inte gjort. [...] Det är otrevligt att hela tiden vara spionerad på. För det är ju det man är. Det är ju hela tiden någon som tittar det är hela tiden någon som hör. Och det är hela tiden någon som kartlägger mig som person.

(I)
Mm jag förstår. Är det någonting som du går och tänker på vardagligen eller är det något som mer kommer upp när du väl pratar om det? Alltså, är det först när du pratar med någon om det som tanker kommer upp eller är det något som du ofta tänker på till vardags när du använder dina smarta enheter?

(U)
Det som, ja det är väl mest när man pratar om det som det kommer upp. Det är ingenting som man går och grubblar på konstant. Sen är det väl vissa saker som man gör för att man inte vill att någon ska ha möjlighet att avlyssna eller ja. Eller se via de kameror som finns i vissa apparater. Tv-apparater, padder, datorer och så vidare.

(I)
Ah okej. Vem är det främst du tänker på när du säger se genom kameror och så?

(U)
Det kan ju vara precis vem som helst. Det kan ju dels vara leverantören som har någon typ av spionprogram inlagt i, från försäljning. Ingen aning. Det kan vara någon som hackar nätverket

och kommer in. Så att det finns ju väldigt många alternativ. Potentiella inbrottstjuvar som vet om man är hemma eller inte. Kan gå in och titta. Se. Kartlägga under en längre tid. Se vart man kanske lägger saker och om man placerar bilnycklar eller plånböcker eller när man kommer hem och man lägger ifrån sig sånt. Även om vi människor är ju lite typ av vanemänniskor. Kommer man hem så kanske man lägger plånboken på ett ställe man lägger nycklarna på samma ställe och bilnycklarna och allting sånt där så det är väldigt lätt att kartlägga.

(I)
Ja men visst. Och om man ser då, ja du nämnde ju lite med att de kan se då hur du lägger grejer och det kan bli, ja att de tittar på vad du gör. Ser du några risker för hushållets personliga integritet vid användning av de smarta enheterna?

(U)
Ja men det blir det ju naturligtvis. Det är ju ändå en följd av att man kartlägger allting man gör allting man säger och kan eller kan göra det. Sen om det görs eller inte det, som sagt jag håller ingen koll på det i med att jag inte eftersökt informationen. Man kan ju kartlägga en person fullständigt. Det har ju kommit fram en och annan nyhet nu på sista tiden som har bekräftat detta också.

(I)
Mm. Vilken nyhet är det du tänker på då eller vilka?

(U)
Ja Facebook. De har sålt massa information till det här engelska företaget och det var ju, jag kommer inte ihåg hur många miljoner facebookanvändare. Uppgifter hade sålts vidare. Och så. Och det är ju bara, bara då inom cituationstecken, bara facebook då som man har kommit på eller identifierat men Google de samlar ju också in information om dig när du är ute på nätet och sådär. Så man kartläggs hela tiden. Och det blir ju naturligtvis då att, ja i kombination med att om man då även kan gå in och se allting i det smarta hemmet då så är man ju väldigt väldigt kartlagd. Man vet ju precis när man går upp på morgon och vad man äter för frukost och när man åker iväg och när man kommer hem. Så det är ju lite granna Orwell 1984. Det var ju en utopi då men det är ju väldigt väldigt verklighet idag.

(I)
Jo verkligen. Men vilken är den främsta orsaken till att du införskaffade dig smarta enheter i hemmet?

(U)

Ja det är väl tanken är väl att det ska underlätta och att det ska spara tid. Beroende på vilken smart enhet man tänker på. Men främst underlätta i vardagen är en orsak. Man tvingas ju även in i användandet av vissa, typ det här kontantlösa samhället, att man inte ska använda kontanter. Tycker jag är staten är orsaken till. Dels minskar man risken för rån i banker, affärer med mera, och privatpersoner får ta ett större ansvar. Och genom det kontantlösa samhället ökar då kontrollen från staten, genom det här kontantlösa samhället. Man förhindrar bland annat det här med svarta pengar i för sig men ja. En del blir att jag tvingas in i det.

(I)
Mm men visst. Och om vi tänker på olika risker då, är det något som påverkar valet av vilka smarta enheter du väljer att använda dig av?

(U)
Ja smarta enheter, smarta funktioner i alla fall. Så att så är det ju i alla fall. Att man inte använder vissa.

(I)
Vilka är det främst du tänker på då när du säger att du inte använder vissa?

(U)
Bra fråga haha.

(I)
Haha.

(U)
Ja det är väl en del program via mobil, mobiltelefonen vissa program där som jag inte vill använda. Jag vill inte ha bank på telefon jag vill inte använda mobilt bankId. Jag tycker man märker att det är alldeles för dålig säkerhet. Och sen finns det ju, det är så mycket med det här trådlös överföring och allt sånt där. Bara det här med keyless bilar till exempel. Man lägger bilnyckeln för nära så, då kan du snappa upp den där signalen utanför och så kan du kopiera den och så kan du stjäla bilen väldigt enkelt.

(I)
Hur, du nämnde just det här med överföring, när man kollar på kommunikation mellan enheter i hemmet. Hur ser du på det? Känns det säkert när kommunikationen sker mellan eller känns det riskfyllt?

(U)

Ja men en signal från en enhet till en annan går ju inte bara mellan de två enheterna utan jag menar signalen åker ju iväg åt alla håll och kanter. Så är det ju. Det är ju inte att man siktar in signalvägen så att den bara går mellan A till B. Från routern till datorn. Utan signalen sprids ju iväg 360 grader. Så att det är någonting som man också ska vara medveten om och det är ju därför man kan, ja det är ju lätt att snappa upp en signal någonstans utanför.

(I)
Ja okej. Men just det här mellan företagen då och dina smarta enheter, känner du ändå att data förs över på ett säkert sätt mellan då, till exempel, företagets servrar och dina system?

(U)
[...] Nej men idag är ju grejen så att idag har man ju inget val heller. Man är ju tvingad att anpassa sig till den här tekniken och till det här idag för att om jag vill betala mina räkningar så finns det inget alternativ att gå och betala räkningar. Utan jag är ju tvingad av bankerna att göra det hemifrån själv. För bankerna hanterar inga pengar längre och jag vet inte om jag kan gå in på ica och betala räkningar på posten där det vet jag inte. Men ja. Så man tvingas ju logga in hemma på banken och sen betala sina räkningar och så. Så att, det blir ju hela tiden påtryckt teknik som man kanske inte egentligen vill ha men man tvingas till det. Det är enklare, visst det är jättenkelt och det är jättelätt och det är jättesmidigt. Men det är inte lika säkert som det är smidigt.

(I)
Ja okej. Jag tänker att om vi går tillbaka till det vi pratade om ganska tidigt, om att du valt att inte kolla upp vilken data som samlats upp kring dig. Så sa du att, nej jag är slö helt enkelt.

(U)
Ja jag har inte gjort mig besväret helt enkelt att ta reda på det.

(I)
Känner du att lätt att ta reda på om du hade velat?

(U)
Det har jag ju ingen aning om eftersom jag inte har försökt.

(I)
Nej haha det är klart. Men, skulle du veta vart du skulle vända dig om du vill veta det? Känns det som att det är något som skulle vara lättåtkomligt rent spontant eller är det att det inte är värt besväret att ens kolla upp för att du vinner mer än vad du förlorar på att använda det?

(U)

Om man säger såhär, det står säkert i den här avtalen som jag godkänner varje gång det kommer en programvara eller någonting sådant där på en miljard sidor. Där står det säkert vilken information som man samlar in och till vilket syfte och ja. Och det vet jag att de gör, men mig veterligen är det väldigt få människor som över huvud taget bryr sig om att läsa igenom det där. Det är så mycket information och det är så mycket text så att man klickar i och sen så har man godkänt och så kan man fortsätta för det är det man är intresserad av att göra just nu. Man vill ju få in den nya programvaran eller man vill ju få in den nya produkten som man just har köpt, då vill man använda den med en gång. Då sitter man inte tre timmar, fyra timmar och läser igenom en jävla godkännande i någon text.

(I)
Ja. Men hur känns det då, hur känner du då när de stoppar in så mycket text?

(U)
Ja det är ju naturligtvis ett sätt för dem att, då kan man ju dölja. Man döljer ju saker och ting lättast helt öppet för då dränker man ju den informationen i en textmassa så att det är väldigt svårt att hitta den texten man kanske då är intresserad av. och så tvingas man ju då att läsa igenom en tjock mängd av text för att hitta det man söker efter. Så det är ju smart av företagen. De får det dem vill, de får den informationen som drar in det dem vill. Jag godkänner bara på rent slentrianmässigt. Informationen finns där, det är upp till mig, men det finns alldeles för mycket text att läsa igenom.

(I)
Mm okej. Och är det då i slutändan, att du använder de smarta enheterna för att du tycker att jag godkänner för att jag vinner mycket på det och det spelar ingen roll att sitta och läsa för att vara säker på det?

(U)
Ja det har väl också det här med slöheten att göra, och man är intresserad av att få igång den här nya apparaten eller det nya programmet som man har köpt eller vad det nu är. Och det är ju det dem vet också. Man är ju intresserad av att börja använda det där. Och därför så godkänner man det slentrianmässigt och läser inte igenom hela texten.

(I)
Mm, och tror du liksom att företagen samlar in data och information om dig, främst för sitt eget syfte eller för dig som användare?

(U)
Sitt eget. Absolut.(I)

Mm, och tror du liksom att företagen samlar in data och information om dig, främst för sitt eget syfte eller för dig som användare?

(U)
Sitt eget. Absolut.

(I)
Ja okej. Om vi tittar på användningsområdena hos smarta enheter: energi, hälsa, säkerhet & underhållning [...][1]. Vilken av de här områdena, känner du personligen, är mest känslig i förhållande till den personliga integriteten i hemmet?

(U)
Det är väl hälsan.

(I)
Varför då?

(U)
Ja för att då är det ju, där är det ju, då letar du ju efter information om att du mår dåligt. Och då samlas det information om att vilka mediciner du har och man blir blottad då i sin eventuella sjukdomstillstånd eller så. Det är ju, är väl mer då att det kanske kan kännas mer kränkande än att någon samlar in information om vilka tv-program jag tittar på. Vilket man gör också i för sig. [...] Jag kan ju tycka att det inte spelar roll om det är långsiktigt eller kortsiktigt. Jag menar, mm man tänker den medicinska biten. Det är ju här då försäkringsbolag kommer in då och kan köpa information och eventuellt neka folk att ta försäkringar och berätta att nej du är alldeles för sjuk för ofta eller ja mycket sånt där. Då måste man vara frisk för att få sjukförsäkring. Och då blir det ju risk för att vissa människor blir utan försäkringsskydd och sådär och då blir det ju helt plötsligt väldiga skillnader i samhället.

(I)
Ja men visst. Nu ska vi se, samma som jag frågade innan med om du visste hur data samlades in. Vet du hur den hanteras av företagen?

(U)
Nej.

(I)
Och har du försökt ta reda på det?

[1]Begrepp förklaras för intervjuperson

(U)
Nej. Jag vet inte, ytterligare kan man väl alltid göra men.

(I)
Okej. Finns det någon orsak till att du inte gjort det?

(U)
Nej det är väl samma som förut, man är för slö för att ta reda på sånt där. Men det är ju, om jag får reda på det så, vad ska jag göra med den informationen? Om jag vet att de lagrar information om mig på det och det sättet, ja det är ju snarast vad de gör med informationen som är intressant.

(I)
Ja okej. Är det någonting du har försökt ta reda på då? Hur de hanterar den?

(U)
Nej. Jag vet vissa företag handlar med information, att det handlas och säljs med sådan information. Så mycket vet jag.

(I)
Okej. Men just kring det då, vad är din åsikt då om hur företagens sätt att hantera den data som de har om dig?

(U)
Ja, nej men det blir ju liksom lite intrång i integriteten. Bara för att jag har köpt en sorts mat en tid så börjar man få rabattkuponger och erbjudanden om just den sortens mat och sådär. Som att man är så inskränkt så att jag ska bara äta den maten i all framtid och kan inte tänka mig att variera. Och ja, det är ju det, på så vis så märker man ju att data samlas in ifrån när man går och handlar i affärer och allting sånt där så att det är, ja det är intrång i den personliga integriteten.

(I)
Men vet du vem som äger rätten till den data som samlas in om dig från de smarta enheterna?

(U)
[...] Ja rätten är väl de som ger ut den här möjligheten eller vad man ska kalla det. För det ingår väl, misstänker jag i det här avtalet som man skrivit på, eller snarare godkänner. Och då godkänner jag, för sen så handlas det ju med de här, den informationen. Det handlar ju folk med, eller företag, med. De säljer ju vidare till andra. Om inte de hade ägt det så hade de inte kunnat sälja det heller

(I)
Mm okej. Vet du vem som får tillgång sedan till den datan som är insamlad och lagrad?

(U)
Ja det pågår säkert rättegångar om sådant haha.

(I)
Haha.

(U)
Haha fråga Facebook. [...] Men, den som betalar för det.

(I)
Och då tänker du?

(U)
Ja den som är intresserad av att köpa den. Företaget, eller ja ägaren då så att säga. Den som samlar in informationen, som jag då påstår äger information i och med att de handlar med den, de säljer ju den. Sen säljer väl dem den till den som är intresserad av att betala för den. De har nog inga skrupler. Sedan finns det ju nu en ny lag som kommer, 25:e maj eller vad är det? Det är EU:s nya lag, hur man nu får behandla personuppgifter och allting sånt där.

(I)
Mm är det GDPR du menar?

(U)
Ja det är möjligt att den heter. Men vad exakt som står i den det har jag ingen aning om, så det kan jag ju inte säga då och skryta med. Jag vet bara att den börjar gälla och sedan om det är striktare eller inte det har jag inte heller någon aning om. Jag har bara fått för mig att det kommer bli lite striktare mot vad det har varit i Sweden.

(I)
Mm, och om man tittar då, enheternas, dina smarta enheter, litar du på att de fungerar som de ska ändå? Eller när du säger att ja, det känns som intrång är det mest främst för externa parter eller från företagen?

(U)

[...]Ja jag har ju inget annat val än att lita på att den ska fungera. Utan det är, så att, så är det ju. Man köper någonting för att det ska fungera, sen vet man ju att det är digitalt och då vet man ju att det inte fungerar i för sig men. Det får man ju, det finns det ju, ja. Men som sagt, man har ju inget annat val än att lita på att det ska fungera så gott det går va.

(I)
Mm. Men anser du då att det finns en risk med att din data kan bli manipulerad?

(U)
Ja.

(I)
Och är det, till vilken grad?

(U)
Ja det beror väl på hur intressant man är som person men någon som vill manipulera kan ju manipulera hur mycket som helst. Så att den kan ju skicka ut kommandon så att det ser ut som att komma från dig personligen men att det är egentligen någon helt annan person som sitter och skickar meddelanden i mitt namn och så vidare.

(I)
Yes okej. Och slutligen då, anser du att enheterna har tillräckligt med begränsningar för olika behörigheter?

(U)
Jag som administratör kan ju naturligtvis gå in och begränsa. Sen har jag ju inte gjort det på de enheterna som jag har men det ska jag ju kunna göra. Det kan man ju, man kan ju begränsa tillgången till de här apparaternas olika delar så att säga. Man kan justera inställningar om jag är administratör, t.ex. på routrar och servrar. Så utifrån min kunskap är möjligheten till begränsningar för olika behörigheter tillräckliga, ja.

(I)
Mm. Yes, men jag tror jag är nöjd där.

(U)
Nej det får du inte vara haha.

(I)
Haha nehe. Men jag får ändå tacka så jättemycket.

(U)
Varsågod.

7.2.2 - Användare 2 (IPA2)

Datum: 2018-04-29, 21:54-22:30
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Då börjar vi. Och jag tänkte börja med att fråga vad din definition egentligen är av personlig integritet? Vad betyder det för dig?

(U)
[...]Personlig integritet det är liksom mer att jag tycker att man inte ska använda mitt namn då så att säga. Att man inte ska bli offentlig med, nej precis man ska inte bli offentlig med sina åsikter, när man tycker till.

(I)
Mm, perfekt. Och då tänkte jag fråga dig också, just det här med smarta enheter. Hur ställer du dig till att de samlar in data om dig?

(U)
Det tycker jag inte om. [...] Ja men nej, jag tycker det är lite obehagligt.

(I)
Mm. Har du försökt kolla upp vilken information som de samlar in från dig?

(U)
Nej jag har inte försökt kolla upp det, utan det liksom har man väl märkt bara.

(I)
Mm, hur har du märkt det?

(U)
Typ på mobilen, att man går och handlar någonstans och helt plötsligt poppar det upp information och frågor om just den affären eller ja.

(I)
Aa. Finns det någon orsak till att du inte har valt att försökt kolla upp vilken typ av information eller vilken typ av data som samlas in från dig?

(U)
Nej det är väl lathet för att man inte vet hur jag ska vända mig för att få reda på det. Nej det inte lathet kanske men ja, jag vet inte var ska jag kolla.

(I)
Mm. Anser du att det är någonting som är svårt att ta reda på då? Eftersom du säger att du inte vet vart du ska börja? Eller är det för att du inte har ens försökt att göra det?

(U)
Nej jag har väl inte försökt att leta upp det heller det har jag inte försökt. Men jag känner mig ju lite maktlös för jag vette fasen vart jag ska ta vägen så att säga, för att ta reda på det. Det är ju inte något, ja är det något, ja man vet ju inte om det är någon speciell myndighet man ska ta reda på som har det eller om, nej jag blir bara förvirrad med hur ska jag ta reda på det [...].

(I)
Mm nu ska vi se. Just det här, du sa att du vet inte vart du ska vända dig med om vilken information som samlar in information om dig. Tror du företagen försöker vara tydliga ändå kring vilken data som de samlar in och hur de hanterar den?

(U)
Alltså vissa företag vet jag ju som typ när man går in på och skaffar appar och allt vad det är, så står det ju då en jättelång harang om vad det ska användas till men jag orkar inte lusläsa och ta till sig vad det är som det ska användas till. Så att dem skriver säkert i den, men de gör det lite väl komplicerat så man orkar inte.

(I)
Aa okej, men känner du att det är deras försök ändå till att vara tydliga?

(U)

Nej det är egentligen inte för att vara tydliga. Utan de gör det bara för att följa regler som gäller för att inte bli anklagade sen. Men jag tycker inte att det är för att vara tydliga direkt utan det är mer för att ha ryggen fri.

(I)
Mm. Men just när företag då samlar in data och använder data som samlas in från dig och ditt hushåll, tror du att de gör det främst för sitt syfte eller tror du att de gör det för dig som användare för att kunna förbättra funktionerna som de är till för att ge dig?

(U)
Det tror jag är både och. Jag tror först och främst att det är för deras eget syfte att de, ja vill kunna göra bättre affär av det hela egentligen. Antingen, ja nu vet inte jag vad för grejer och olika produkter, men göra reklammässigt så att de kan nå ut till mera företag då så att säga kanske försöka komma in i det hela men självklart kan det ju också vara en del att förbättra produkter, så kan det ju vara. Men jag tror mer på nummer ett då, först och främst.

(I)
Mm okej. Och om vi tittar då när du använder dig då av smarta enheter, ser du någon risk för hushållets säkerhet av den personliga integriteten för ett helt hushåll, vid användning av det?

(U)
Ja det ser jag. Ja framför allt typ när det är kameror i hemmet, där det är många som är filmade och det går ut på nätet. Och det är inte säkert dem som är i hemmet som vill det.

(I)
Mm. Är det då för själva överföringen av data då alltså som du syftar på att det är just den kopplingen som är osäker eller är det är någon, att det är för lätt att komma in på nätet?

(U)
Ja det är lätt att fel personer får tillgång till det [...]. Jag kanske då som kund vill använda det här då för att jag själv ska hålla koll på någonting inom mitt hus. Och i och med att det finns många då som kan hacka sig in, ja då kan det användas på fel sätt bland annat.

(I)
Mm. Finns det någon orsak till att du känner att det är så sårbart? Eller så lätt att bryta sig in på?

(U)
Ja alltså erfarenhet av, för min del, så tycker jag bara det att en enkel sak att ha saker på ett moln så att säga, eller ja i cybern, jag får av erfarenhet andras bilder till mig. Då kan jag ju bara gissa,

var är mina bilder någonstans? Vem har fått dem? Jag kanske inte har alla bilder på mitt moln då så att säga. Så varför ska inte det kunna vara så med alla andra grejer också.

(I)
Mm. Så den här typen av risker, eller ja de riskerna som du ser, påverkar de valet av vilka smarta enheter och funktioner som du väljer att använda dig av då?

(U)
Absolut. Det gör det. Det måste det. Det får inte vara någonting som kan vara en risk med, som kan påverka mig ja, kanske ekonomiskt eller ja, som skulle kunna ge skada för mig.

(I)
Mm. Skulle du kunna förtydliga vad du menar som data som inte skulle skada dig?

(U)
[...] Ja, skada i för sig det gör det ju inte. Man kan ju säga såhär menar, det skadar inte mig om någon annan får veta vad jag äter och ja, typ sådana saker. Det är ju klart att det inte skadar mig men samtidigt så vet jag att man kan bli terroriserad av företag då som vill sälja på mig reklamprodukterna. Så att det är klart att det finns mycket som inte skadar mig men det kan bli jobbigt av det istället. På min fritid till att göra vad jag vill utan tanken är ju då att skicka massa erbjudanden via mail eller telefon eller sms, ja.

(I)
Yes. Och när man tänker på smarta hem så, man kan då dela upp det i fyra olika områden. Och det är då underhållning, hälsa, säkerhet och energi [...][2]. Vilket av de här områdena skulle du anse mest känsligt i förhållande till säkerhet av den personliga integriteten? Och varför?

(U)
Det är ju låssidan då så att säga, på grund av att kan jag då sitta på andra sidan jorden och låsa upp dörren så kan någon annan sitta och låsa upp dörren utan att jag vill det så att säga. Så den är ganska enkel och så. Ja.

(I)
Ja okej. Och det är även då när du tänker ur personlig integritet som säkerhet är det mest känsliga?

(U)

[2] Begrepp förklaras för intervjuperson

Ja det är mitt innersta haha, eller vad ska man säga, ja jag har svårt med ordet men, ja men det är ju den. Det här med musiksmak och det är ju nej, nej men låssidan. [...] Jag kommer alltid vilja ha säkerhet så att inte någon ska komma in mig på livet som jag inte vill ha här på något vis så att säga.

(I)
[...] Mm okej. Och just med de smarta enheterna som ni använder trots vissa risker som du då själv tycker att det finns och som man hittat, fortsätter du använda enheterna då för att du anser att vinsten är större än riskerna vid användning av dem? Med den typen av enheter som du själv använder idag?

(U)
Jag tror att jag använder det vidare för att man orkar inte ta steget ur det, för att det här använder alla mer eller mindre. Och även om man blir räddare och räddare för att använda det just för att de plockar på sig så mycket information av mig som jag inte vill att andra ska ha så är det ändå svårt att ta sig ur det för att, tar man sig ur en grej så måste du ha en sak kanske och då måste du gå med på det i alla fall. Du blir lite intvingad i det. Eller ja inte lite, man blir intvingad i det för att du har inget val. För ska du ha ett hjälpmedel så att säga eller app, ja då är du ju tvungen att acceptera det här och då, ja till exempel vill du inte ha Facebook nu, ja då är det massor med andra grejer som gör att ja, då kan du ju inte använda vissa saker. Jag känner mig tvingad.

(I)
Ja okej. Vilken är från början, om man tittar, vilken är den främsta orsaken till att du skaffade dig smarta enheter i hemmet?

(U)
Ja det är ju lite spännande med nyheter haha.

(I)
Haha jo.

(U)
Haha så är det ju. man ser ju inte nackdelarna kanske på en gång på det sättet utan man vill ju bara se det braiga i det. Men det är ju smarta saker många gånger, så man har ju glädje av det. Bara det att man, det är ju avigsidan. Men visst är det smart att ha det här, att kunna ändra belysning och sånt när man är borta och höja sänka värmen i sommarstugan och om man är i närheten och så, ja visst det är ju jättebra men sen, ja. Det är väl det som gör att man nappar på det hela.

(I)
Mm, och vi pratade då innan om att om du hade kollat upp det här med om vad för data som samlades in av företagen, vet du hur datan hanteras och lagras sen från företagen?

(U)
Nej inte det minsta.

(I)
Är det någonting du har försökt ta reda på?

(U)
Nej det har jag inte. Det är samma där, jag känner att det, man inbillar sig det är ingen idé att hålla på och söka för, var ska jag söka. Det är så invecklat när man ska, så fort det blir just den här olämpligheten. Man slutar. Man kan ju googla ihjäl sig jag menar på enklare saker när man ska hitta hjälp då och prata med någon eller få svar på någonting. Men det är liksom, man ger nästan upp direkt innan man ens försöker få reda på en sådan grej.

(I)
Mm. Vet du vem som äger rätten till den data som samlas in av de smarta enheterna?

(U)
Ja alltså, jag vet inte. Men ibland så brukar det ju, jag tror det brukar kunna stå det företaget äger rätten då eller, om man nu säger Spotify eller vad det nu är, att godkänner du det här så äger de rätten till att använda sig av information då så att säga. Så det måste ju vara företagen då så, ja det är så jag uppfattar det som i alla fall.

(I)
Mm, vet du vem i så fall som har tillgång till den insamlade datan?

(U)
Nej. Inte mer än företaget i sig då. Inte för att jag har kollat det.

(I)
Aa okej. Och hur ställer du dig till att det är företagen som äger rätten till data om dig?

(U)
Nej jag tycker det är hemskt. Jag tycker varför ska de äga rätten till det? Jag tycker det är fruktansvärt. Det är, jag ska väl få äga rätten till mina åsikter och information om vad jag gör eller inte. Det är det ingen annan som ska göra. Bara för att jag använder en produkt så att säga.

(I)
Mm. Och om vi då fortsätter sedan då på att informationen sedan överförs, den data som har samlats in, den samlas ju in från enheterna och sedan så överförs den mellan enheterna för att göra dig hem så bekvämt och funktionellt som möjligt. Hur ser du på kommunikationen som sker mellan de smarta enheterna? Och hur ser du på kommunikationen mellan de smarta enheterna och övriga system som hanterar datan, som exempelvis då kan vara företagens servrar? Alltså litar du på att datan överförs på ett säkert sätt mellan dina smarta enheter och exempelvis företagens servrar?

(U)
Nej.

(I)
Varför inte?

(U)
Ja jag kan väl gå tillbaka till det där med the cloud och så, helt plötsligt kommer nya foton som inte är mina foton. Alltså det är, jag tror det är för stort för att företaget ska vara säkert på att klara av det på grund av att man ser bara bankerna, jag menar bankerna har problem att klara av det och de vill väl om någon. Att pengar inte ska försvinna i cybern så att säga. Det är givetvis alltid kryphål känner jag. Nej så jag har svårt att lita på det, jag litar inte ett dugg på det. När jag tvingas att lämna ifrån mig uppgifter då gör jag det och känner att nu vet man aldrig när det kan hända någonting. Det är inte känsliga uppgifter kanske alla gånger, men känsligast är ju då sähär med lås och bank och hela den biten.

(I)
Aa. Har du då funderat någonting kring på vad som tänkas, vad det kan tänkas användas till i framtiden?

(U)
Ja diverse scenarion kring kriminalitet. Fel personer får användning till att plocka saker av folk och använda det till fel saker så att säga. Inte för att gynna sin konsument, och nu menar jag att inte företagets ska skinna en utan att någon hackar sig in då så att säga för att ja, till att göra inbrott, plocka, ja nu tar jag samma saker hela tiden känner jag.

(I)
Nej men jag förstår absolut. Men anser du att enheterna har tillräckligt med begränsningar för olika behörigheter? Just det här då till exempel med kodlås då att du som admin kan begränsa

andras behörigheter? Säg på till exempel smarta TV-apparater kan du då begränsa så att barn inte kan titta på vuxenprogram? Anser du att den typen av begränsningar som finns, är den tillräcklig? Och nu pratar vi ju då i förhållande till säkerheten av din personliga integritet när du använder dig av de smarta enheterna hemma [...].

(U)
Nja kanske inte riktigt. Inte riktigt hundra för att om jag nu bara tänker vad jag har för grejer så, något som då också har med integritet som larm och sånt där, jag menar att man får, de koderna de ska ju då larmcentralen ha. Och då ska jag lita på, jag är ju tvungen att lita på larmcentralen att de har folk som inte gör någonting med de där koderna. För de är ju, det är inte tillräckligt för att jag kan ha en extra kod så att de inte kommer in på grund av att de inte har den sista koden. Där finns det ju ingen gräns utan de har ju exakt det jag har. Eller typ när man gör en kod till, ja vilken sida som helst så att säga. Den koden, antar jag, får ju det företaget. Även om de ska säga att de inte ska skicka ut den. Men någonstans så måste ju de se den koden och vad det händer med den, ja det vet ju inte jag riktigt. Så att jag vet inte, nej det känns inte tillräckligt.

(I)
Mm okej, men anser du att din data är alltid tillgänglig för dig när du behöver den?

(U)
Är man envis så kan man säkert hitta, om man luskar. Men det är inte så himla lätt. Men en del har jag väl lyckats med när jag väl luskar. Men det är krångligt att leta sig fram till det, det är mer en slump till att man kommer på det. Inte för att man kan hitta på allt, men ja. Vissa grejer kan man ju hitta. Men det är främst tack vare hjälp av yngre.

(I)
Mm, men då, litar du på att enheterna fungerar som de ska?

(U)
Som vilka varor som helst alltså. Ja för det mesta ska det väl fungera sen, ja finns det väl fel på allting. Någonstans finns det ju alltid någonting som kan gå fel, men för det mesta ska det väl fungera. Det ska det väl. Säger jag då. Men jag litar inte fullt ut på dem, det gör jag inte. Det går inte. Hundra gör jag inte, men man blir så illa tvungen till att försöka förlita sig på dem. [...] Jag måste säga att det ofta är jobbigt. Jag tycker det blir mer och mer grejer som blir på det här sättet så att säga. Mot vad det har varit förut. Och det blir mer, vad säger man, smartanpassat så att säga. [...] Som sagt, det finns ju inget system som är hundraprocentigt. Men jag tycker det känns för okollat på något vis. Jag vet inte vad jag ska använda för ord. Det är många gånger så börjar det användas system utan att verkligen ha någon, det känns som att det inte är tillräckligt stark bakgrund för att vara säker på att det verkligen fungerar.

(I)
Ah okej. [...] Om vi spinner vidare på det vi pratade innan om, hur datan sparas och lagras, anser du att det finns risk med att den kan bli manipulerad?

(U)
Ja för vad, hur ska jag kunna säga att det här stämmer haha. Jag vet ju inte ens om att det sprids och hur det sprids och till vem det sprids. Och vad sägs om vad jag gör eller inte gör. Det finns ju inget ställe jag kan kolla det. Är det bara någonting då som bestäms, så det här ska du acceptera, nu använder vi det här. Och hur, som sagt var, hur det används eller till vilket syfte exakt eller nej det, det har man ju ingen koll på.

(I)
Ja, nej. Ser du det som ett problem då?

(U)
Ja haha, absolut. Absolut. Det finns ju mer nackdelar faktiskt med det hela än fördelar. [...] Problemet är ju väl att det ändras i siffror då kanske om det är en som gör ändringen, eller oavsett om det är medvetet eller inte, gör att jag kanske blir då, i min värld, trakasserad av nya försäljare eller om jag som företag har fått fel uppgifter som läggs ut i nätet som jag inte har någon aning om, det påverkar ju min kundkrets till exempel. Dåligt. För att, ja vad det nu må vara då om det nu inte stämmer med, telefonnumret kanske är inskrivet fel, ja då når de inte mig. De tror att man har slutat, jobbar inte längre på det här sättet eller så att nej jag kan inte liksom ha den där kollen. I och med att jag har inte den blekaste aningen vem av alla dessa som har rättigheterna då. Vem gör någonting fel, det är helt omöjligt. Och det påverkar ju mig, troligtvis mest till det sämre. Det är inte positivt i alla fall.

(I)
Yes. Men jag får tacka så mycket.

(U)
Väldigt negativ person men ja varsågod haha.

(I)
Haha nej men jag är jättenöjd och får tacka så mycket till att du har tagit dig tiden till det här.

(U)
Ja det var så lite så.

7.2.3 - Användare 3 (IPA3)

Datum: 2018-04-30, 21:27-22:27
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
If we start the whole thing looking from your point of view, what would your definition of personal integrity be?

(U)
[...] It would be the impact that has on my personal information and given the information or given out, that would be if it came back to me via third party. So if I felt like I was getting other people contacting me on the back of the information I've been given to my smart company, that would be how it affect me. But personally, it doesn't bother me. Otherwise, apart from that. Does that make sense?

(I)
Yeah definitely.

(U)
I would only think I've been manipulated if they use my information for advertising and other things [...].

(I)
Yeah ok. [...] So how do you feel, as a user, that the devices are collecting data or information from you?

(U)
Well yeah very much, they do take a lot of information. I didn't realize they that, if I look at my motion detector now, it will tell me when the last time that the detectors sensed anyone moving

in the house while I'm at home now so that will now tell me that I've been in the house for however many hours. So that now is my movement as well as anyone else who comes in. If you see what I mean. Well that doesn't have my motion, but that doesn't, well I know my motions because obviously I can look at it and it actually records all the days gone back for weeks. So I can look at all that information, so that's a little bit intrusive in a way but that's what I wanted it for. So I'm not criticising the way they collect that data because what I put there I would'nt know. Because if I wanna think who came in my house yesterday, if there was anyone in my house for 4 hours yesterday, even if I forgot to turn on my sensor when I went out, that would still tell me. That just wouldn't send me a text message if I hadn't switched that on but it still records all the motion in my house all the time I'm there or not there. Yeah. Which is quite handy when you've got people in there that you don't want to come in your house when you're not there, if you know what I mean. Yeah, so it's quite good. But what is quite funny is if the postman puts letters through the door, I sometimes will get a text message if the letter gets flowing through the door, haha, and moves, I get text messages saying there is motion. But if I think there is anyone in the house, that would, I could look at the app, I can actually look at it and that data builds up, and that will then tell me that if there is still people moving in the house. But if there is just a mail, that will land on the mat and then it won't move anymore so that would be just for one time. That's quite clever yeah. But I don't mind, you know I don't mind the fact that that's what they're having to do to sense it, because that's what I've asked for. That's what I've bought in to. But I don't know what data they collect, it must all be done by, I'm not sure how it works really.

(I)
Yeah ok, so you don't know exactly what kind of data that the units are collecting from you?

(U)
No. They would be able to detect things like my electricity use if I'm using the bulbs but that's' all. They can't detect much else from there. But if I had, I don't know if I would want a camera, but if you have a camera I'm not sure, if you can see the images in your house I don't know if anyone else would be able to see them as well because, do you see what I mean?

(I)
Yeah.

(U)
So that does information about who's moving inside of my house, obviously because that's sending me a message. But they can't see in my house, but with the camera, if I could see on my phone who is walking around they must be able to see, someone must be able to see that as well I guess.

(I)
Yeah.

(U)
So that's probably where it gets a little intrusive.

(I)
So, like the security risks that you are talking about right now, is that a reason for why you're not using some devices? Because that kind of risks will come or?

(U)
Yeah it could be. But I think I've got enough safety devices here to what I need and what I pay for, because you need to pay for it. And so the more gadgets you buy, the more light bulbs you buy to switch on and off and the more sockets you buy, the more motion detectors you have in different places in your house, you pay more for the gadgets. So I feel I'm more, I've mainly gone for what I need, to suit my needs. You know you can get five, six motion detectors if you've got a house which has lots of corridors and different rooms but everything in my house goes from the hall. So anyone who comes in, to go upstairs or through the lounge or through the bac, through the kitchen they would have to come through the hall. So I only need to have a basic system to be, to tell me if there is anyone there. But I guess if you had more detectors, they get more motion detected, they would have more data on file wouldn't they. Different points yeah, but I don't know. It's all linked to the same system but they're also doing window detectors and you could even have them connected to your windows so if a window gets opened you get a text message to tell you. But only think how many windows as you've got in your house, or doors, you need quite a few. But if anyone is gonna come through the windows, they would walk through the hall anyway. Yeah, but I don't really know what they keep as far as, or what they need to, you know data wise, to set this up. They've got my E-mail, my phone number, as far as I know that's all. Oh no, and my bank account obviously. Because they got, they take money for it for every month.

(I)
Yeah ok. Have you tried to find what information they're collecting from you?

(U)
No. Yeah, no.

(I)
Ok. Is there a reason for why you haven't?

(U)
I'm not that bothered about it really. I don't think that, you know, I always think that comes with it you know, with the package. If you want to have something, that's the trade off. You need to have a, you need to give them certain information don't you. So that's a lot of, there is a few years ago there was a lot of worry about the information you were giving them to connect to your, it's called a hub isn't it?

(I)
Yeah.

(U)
The information they could collect from your hub because that was linked to your modem and stuff, it was a little bit, who has decided they can't link in to your other details if it's connected to your wifi. So that's the big problem with people who were a bit sceptical about it. They were saying all "oh no they could get if you've got a hub connected to your wifi, which is obviously all linked to your system, they could get in to your bank details and computer systems". Which might be more of a problem if you're a business rather than a house, if you see what I mean. Yeah, but there has never been any proof that that has ever happened to anyone. But if you move, if everything is connected to you phone sorry, if your phone is connected to your, not your phone sorry, so your hub is connected to your wifi obviously, potentially I suppose they could, someone who's a bit of a hacker could get in to your system, but I don't think the companies obviously do [...]. They wouldn't do that, I don't think. But probably what they call a hive, terms and conditions, probably tells you about the data protection that they use. But I wouldn't honestly tell you what it is. What protection they would set in place to safeguard your security. You can probably find that out, wouldn't you, online.

(I)
Yeah probably they do, yeah.

(U)
Are you getting people who think that, that doesn't you know affect their integrity on the way that the information is being used [...]?

(I)
Yeah, there is definitely a mix of it. Like, quite a big mix of people yeah.

(U)

Yeah. The first time they brought out the heating one, the heating app, the big objection to it was that, they used to sell it as a part of a, an add-on for central heating system, was to control it remotely from an app anywhere in the world. And the biggest complain at the time was that now I would have to give everyone my information and they'll know where I am and what I'm doing. So they thought that if you're inside Australia, and you start switching on your heating from Australia, they could know where you are haha, while to me that's no different from sending someone an email or so, they're getting the information the same way I guess. That's beyond me how it works haha.

(I)
Haha yeah I guess that's true. So do you the companies are trying to be clear about what information they are collecting and how it is handled from them?

(U)
Yeah, yeah the more information they get on you, on the usage in your home, then yeah I think it leads to more further development to other products really. So if you know for instance that I'm in the house 19 hours a day, every day, they are more likely to wanna sell me something for the house, than if I'm someone who's only in for two hours a day or you know, just using the place as a base or something. So yeah, yeah they do. It's a bit like if you go on Amazon and you start looking at books, five minutes later you get a pop-up saying "books you might be interested in" and you're thinking well, they have got that from my browsing history haven't they. So I think it's how it works with the smart stuff as well, yeah they will see how you use your equipment and they will probably be offering you products to make it a bit easier or a bit, yeah products along the same lines.

(I)
[...] Do you believe that it's mainly for their winning or for you as a user? I mean, like you say they're sending you offers etc.

(U)
Yeah, I wouldn't really, I wouldn't be the sort of person that would buy much extra because they sent me an advert based on my usage. That's just clever marketing, isn't it. That's no different from when you go in to a shop now and you use a loyalty card, and they know exactly what food products you buy everytime you go in. So you go in with your loyalty card, and then a couple of weeks later you get an offer like 5:- off something because you're normally buying that thing. That's a smart device in a way, and that's where the marketing has changed around you get adverts based on your shopping habits, what you buy. So if they know you buy wine every time you go in, if they offer you 5:- off you're more likely to buy another bottle haha. So I very often don't bother to use my loyalty card when i don't spend much money because I don't really want

them to know what I'm buying. That's just, see I'm just finding that more intrusive when I've just gone shopping and coming back to me a couple of weeks later and you know sometimes they're quite good but normally that's just a little too close. You know, too close on what they're remembering, too close on what information they've got on you. Smart cards in a way, isn't it?

(I)
Yeah for sure.

(U)
Yeah.

(I)
So if we go back to when you were talking about the possibility for hackers or when the data is secure, when you talked about your information, bank details and stuff. How do you look at the communication between the units, like between your smart devices and your phone for example where you're controlling it from? Or between your units and the company's servers? How would you look at the communication between them, like the transfer of data?

(U)
You know what, the information is just, that's just telling me what I've asked for really. They give me the information I've asked for, I want them to tell me if there is anyone in my house. So that transfer of information is just, to me, that's no different from just somebody just, was in my house and said "somebody lives here" and said "somebody now walked in the front door" and phone me up or texted me to tell me. So that's just their way of doing it without anyone being inaccessibly and to deter it for me, so I quite like it, so, I don't really, that doesn't cause me any problems but the data they gather to do that is obviously an essential part of how it works. If they couldn't sense there is anyone in my house they wouldn't be able to tell me, would they? So how it works, as I said, the technology and the sides of it I'm not sure, but what data they would collect above and beyond keeping me, just letting me know what's happening I don't know.

(I)
Yeah. Do you trust that the transfer is safe then?

(U)
Yeah, I do. Yeah. Otherwise I wouldn't have it. But there is always that risk that you don't know. There is always that, you know, possibility that how things get hacked is because of something that you wouldn't expect. So I used to have a front door bell, so if anyone rang my front door bell, I just got a ringer inside, a remote one so a wireless one, but because it had a signal, an infrared signal, what used to happen occasionally would be my door bell would ring

and there was no one at the door. Because if somebody else came passed my house with the same frequency from a, like a key fog for a car, that was the same frequency, and it set off the door alarm. So even that was a sort of smart device, that wouldn't, necessarily be working solely on that one. But there must only be so many frequencies they can have for that door bell to work. So same what happens on that, you know I used to go to the front door and the door would be ringing but there would be no one there. So you get that sort of technology based on, you know information gathered like that. So it was the same there, it could be a security risk. That people realise that by crossing your doorbell, they could probably get in to your car because the car is now a days keyless aren't they. So you could press the button, and the infrared opens the door, if someone that has got a similar control for something else that have an infrared device, same there for bluetooth device, they could get in to your car. Yeah that's another one, did you know about the keyless cars now? If you've got keys in your house, you should really keep keyless car keys in your, oh they're not keys they are buttons now aren't they, you should keep them in a metal box so that they can't get hacked. Because anyone with the right device could stand outside your house, if your keys are sitting on your window seal inside your front door, they can get that code from your phone, from your keyless activation system and open your car. And steal your car. People have been told now put them keys, that particular type of key in a metal box so that they don't radiate the signal haha. It's another smart device which is why people are a bit worried about anything else that is them sorts of devices, it have been proven to, you know if you have the knowledge on how they work they can start to steal cars. That's the data they pick up from your key folders, transmitted on to their own device to let them open your car. It's a weird eesystem isn't it?

(I)
Yeah haha. It's a funny system.

(U)
Yeah. Another thing is, when I share a Spotify account with [...] and she has got, she obviously got access to the Spotify account, but we can only play it one at a time. So when she is listening to the music, I can't listen to it at the same time until she is finished. Yeah, so if I'm at home and I want Spotify, and she decides to go on hers' and turn it on, she stops my music from anywhere in the world haha, that's ridiculous. Another smart device that must take your data and take it, or at least to set it up on to a new account so it's just stops mine and starts hers'. So hers' got preference over mine for some reason. [...] Yeah. Well I see all of these like smart devices, I see them more as a, like a bonus really. Just to me, things like remote access for burglar alarms and stuff, without any wires, it's brilliant. Cause years ago if I wanted a burglar alarm in my house or a camera, I would've had to wire it all in and that cost, it used to cost a lot of money. Now you can pick up a smart device now, which is all wireless stuff. So the trade-off aren't, on that is, potentially I suppose yeah someone might be able to get more information or data from the

system about whatever it's connected in to. But I'm happy with that because that allows me to have a relatively cheap security device. That wasn't the case before [...].

(I)
Yeah, yeah it definitely is. Yeah, you're answering a lot of my questions. This is perfect. So, do you know who owns the right of the data that is collected from the smart units?

(U)
Hive is owned by the British Gas. That was always their technology, the Hive system. Initially that was just British Gas selling an app on your phone which allowed you to turn your heating on if you forgot to turn it on or turn it off from your phone anywhere in the world. But then they've now started to, all these devices, with gadgets like phones and all sorts of things but you can buy the hive system in lots of shops, their shops now. You used to be the only people who, that used to sell it because they were British Gas. But then they realised that if they sold it to the shops, so the shops became their agents. And again I suppose that opens up another line of who has got access to your information if you went in the shop to buy it. But the truth is that you buy the kit from the shop and you go home and set it up yourself. With Hive, this is like copyright company itself. But I don't know who own the other ones, I know the company called Nest does a similar thing but I don't know who owns that. But I know British Gas owns the Hive system. So you would like to think it would be some come back if anything goes wrong or, you know if anything goes wrong that you've been told that there is someone in your house and there's actually, there was, and if you weren't then told and there was someone in there. You would have to put the comeback on that. And then yeah.

(I)
Yeah, so you mean that, for example, that it's the company then that owns the data that is collected? Or is it, would that be you as a user, that actually owns the data that is collected?

(U)
Yeah, they would collect it yeah, they would keep it. They used to use the central heating system information for finding out how old your boiler was.

(I)
Ah ok, yeah.

(U)
So if you thought, like set up your central heating thermostat to say, my heating is gonna come on if I go to work in the morning and forgot to turn my heating on, I can turn it on on the phone so that doesn't waste gas all day. But when they set that up, some of the questions they would

ask you would be, they would ask you a question like “Is, how old is your boiler?”. And if you asked them why they needed to have that information, the answer would be because if it’s over a certain age that won’t work. But the information, that’s how the technology won’t work with an old boiler. But in truth, the reason why they wanted to know you had an old boiler was they can then target you with marketing to sell you a new one.

(I)
Ah yeah haha, smart.

(U)
They were after information rather then the data that was there about there at the time. That was questions leading for a future marketing. And they would gather of knowing ruffly on how old peoples heating systems were. So younger people tended to go for smart devices while the older people wouldn’t want them. But very often the younger people had the new boilers. So once they sold them a new boiler, they would normally sell them a smart device to control it. So they hit you with two sales in one haha. It’s just marketing, it’s just sales isn’t it. It’s just an add-on really, but a lot of these smart devices started off as add-ons for other things. And they’ve now become the norm really so you can actually get a complete smart house now, can’t you. With, I don’t know, remote curtain tracks and to open and shut your curtains and turn your radio on through the, I can’t remember what it’s called now, but the device that comes on your Amazon?

(I)
Alexa?

(U)
Alexa yeah. That’s one of them. That’s what connects, that can get one of them as well and spin it to my Hives control. The small one, I don’t think it’s the Alexa I think it’s the other one, it’s the one that connects, without me even needing to be bothered to get off me seat I can get the television to turn on.

(I)
Yeah, do you mean with the Echo hub?

(U)
Yeah Echo dot, yeah that’s the one. Yeah that can controls the whole Hive as well. So you can, you can actually sit at home and say “please turn the lights on” or “turn the radio up” or things like that. But you just need lots more smart devices to make that work. You can’t just tell an Echo device to open your curtains because it’s not controlled electronically unless you have got a device which is all set up to do it, so. It’s not very often, it’s very much, a lot of the information,

the technology is still in its infancy. So that's acts, you can do all these things but a lot of acts spending a lot of money on, on the controls to make it work.

(I)
Yeah, yeah the technology is definitely moving fast.

(U)
Yeah it is, yeah. So what you need to be doing is to asking yourself what it's gonna be like in 20 years time. And then all the information is, all the data they're gathering now, will be used to prove how all these devices work. Well everything when I was younger was all wired, wasn't it, everything had to be wired in. And then suddenly everything became wireless. And now it's all bluetooth isn't it. So where is the wireless would only work within a certain range, and then the bluetooth works anywhere in the world.

(I)
Yeah that's true. That is both handy and a bad part about it. Always pro's and con's from it.

(U)
Yeah. But what's next we don't know do we haha.

(I)
No not really haha.

(U)
No. Well the houses that are getting built now with all the smart devices in them so as long as you, if you build the house in the first place with all the infrastructure, all the kit they [...] the bluetooth in and the devices that allow you to do things like, I don't know, curtains or something. With that they don't need to do it later, that makes it like a lot easier. You know they'll build the houses with smart controls now, and if I look on mine now to see if I want to buy a new house. I'm looking to sell mine, lots of the adverts now mention the fact that lots of the houses come with smart devices. Yeah so they advertise, big advert for, I can't remember the one I read now but there is quite a few now. Obviously the central heating controls and the remote, the remote things like garage doors and bluetooth operated garage doors, not garage doors sorry driveway doors. Electronic doors. So as you drive up to your gate, your gate automatically opens and the garage door opens behind it and you can get in. straight in to your gate, straight in to your garage and everything closes behind it. I mean your light switch on when you enter your house but they, there are a lot of, estate agents use that now as a selling point for a house. Smart devices, yeah. That's not why I've got mine but that does make sort of like a bit easier to sell your house. So if you've got that and an identical house hasn't so. It's a bit of a selling point.

(I)
Yeah exactly. So do you see any risks for your personal integrity while you're using smart units, out of a security perspective?

(U)
Yeah. Yeah I do, yeah. Potentially there's the risk that my information will get used for other things, yeah. But I haven't had any, I've never come across anything. That trust has never been broken up until now, but that is obviously one of the things you think about while setting this thing up.[...] My biggest risk would be if I found out that they, got hacked into my computer and got my bank, online bank details. So if they could hack into your bank details because of, through, somehow through a hub that you're using. Now I don't know if they can do that or not or if the technology is out there for people to do that but potentially there is yeah. I've got a mate [...] who works in, he works in security, not security. What's his class, he is an accountant. He is a forensic accountant, so he deals with insurance claims which, they have to ascertain if the insurance claims are fraudulently been put through or correct. So if someone says they've had their 100:- nicked out of their pocket they would pay it out. But if they say they've had 18 cars stolen from their garage, they would then look in to it a bit more. You know what I mean, so the bigger claims, bigger claims go through forensic examiner first to make sure that there is not people just trying it on. You know with the whiplash injuries and things like that they need to make sure that they're genuine or there will be these companies that comes to them and say can you just check this one for me to see if this is genuine. And his job is based on a lot of security on information like that so he is, he had to go to a seminar the other day where the bloke who is a hacker, like a professional security hacker for companies, for companies security. And he said all he needs is, to getting in to someones system is their phone. So if anyone gives him their phone, you know within 10 minutes or so he reckons he would normally, 99 percent of the time, get the information he needed to get in to their bank details and clear their account.

(I)
Oh wow.

(U)
And if that is that business, he works in the corporate side, so if that was a business he is dealing with, he could sweet talk his way into a dinner with, say the chief executive, be in a lunch with him and say "Can I just borrow your phone because my phone has died?". So he would give him his phone and then by, to see what his password is, then they can make up they are making a phone call or text message, he would be able to go through that blokes phone and find out all his bank details and clear his account. So that the company, he can even literally close the companies down with the information that he, he knows how to work on a system. So all that he

needed is someone to lend him a mobile phone and he is laughing, and [...] said he doesn't know how he does that, he said, but that's what he does.

(I)
That's crazy yeah.

(U)
Yeah, so people employ him to make sure that the companies are one step ahead of the hackers. Because then he need to tell them how to protect their systems. But he said the first way he normally does is just prove to these people that he is already in to their account when they're, if they're thinking about employing him haha.

(I)
Haha.

(U)
So yeah, that would be my worry. I think that if I lost my money at my bank account or all of the things like, yeah, I don't know. That would be the worst thing would it, getting money wiped out from your account. That's all that count, is where you held the money is it? So if that was proven to be taken, because someone had Hämtad any information from a security point of view, because my reason I've got smart devices is the 100 percent security, really. It is not about being lazy, getting off a chair to turn the light on. That's about the ability to be able to switch the lights on and stuff on from anywhere else to make my house safe. So from a security point of view, if I got hacked because of that, then yeah that would be my worry. But that would be an annoying thing really, because it's the main reason I'm buying one of these things in the first place. But as I said that's the trade-off to me, either you buy them or your don't buy them. And you take the risks of potentially more data fraud against you, or you don't have them.

(I)
Yeah that's true. So if we go, if we stay within the area of the question, and the, 'cause if you look at smart homes you can say that they're divided into four different areas: energy, health, seurity and entertainment [...][3]. What of those areas would be most like vulnerable towards you for the security of your personal integrity? Like if someone could reach that data?

(U)
Yeah I see, well that would be the security because that's what I use the most of. The entertaintment thing I, it don't got much on you there, it knows what music you listen to. It's not

[3] Begrepp förklaras för intervjuperson

much it's, it's just Spotify. Unless you've got things like, I don't know mySky is all bluetooth isn't it? So that's linked in to your wifi but, nearly everyone in the world is on that now aren't they. So yeah, so that's smart device isn't it. Yeah it is, because mine is wifi from the other room from, from Sky. So that's linked into my modem. But no, I would say the integrity would be more at risk with my security system so I haven't got anything on the health side that uses the smart devices so I don't got a fit-bit or anything. Any entertainment, yeah I have. What was the other one?

(I)
Energy.

(U)
Energy yeah. No, well, not really no. Unless mine come over to energy because I do plug-in, I do plug-in heater. Just in to a socket, so if I think that it's gonna get cold I can still have one room warmed up on a heater. Not the central heating system but I can have a heater plugged in, but that wouldn't really affect me I don't think. It wouldn't worry me so the security side would be. So I think the security side links to your, not just the smart security I've bought in to, I'm talking about the security of your phone oh sorry of your bank account at the same time. So that security actually goes in two in different ways doesn't it. And the security that you bought for your protection and your security that is giving them data wise, will affect your personal security. You know your bank details and your computer information and stuff. But only if you've got something to hide haha.

(I)
Haha yeah exactly.

(U)
I think I'm too boring to have much that people would find very interesting if they turned my laptop on. Mine would only wanna come in to my bank account yeah, so obviously my browsing history that's probably a bit of Facebook and yeah and a few chats on messenger. Yeah that would be a bit boring I think. And what books I've read on with Kindle, yeah. They would switch mine off and move on to somebody else haha. Yeah we probably all think that, don't we.

(I)
Haha yeah probably I guess so.

(U)
We probably don't think we are particularly different from anybody else but, you know. Yeah, I don't know. But the cybercrime is all based on money isn't it. So that's like the banks, when the

banks get hit don't they and they say all the 5 000 accounts have been hacked is today because of a security link. And i think that's the companies that are more at risk of being targeted than them targeting me with the information I've given them. So I don't think my problem would be with the company I'm buying the stuff from, that's more about the people that are trying to hack in to the companies computer systems. And that's where everyone is more worried. Yeah, 'cause no one really minds that much if you get a company trying to sell you something knowing that you buy the same bottles of wine every week or, you know you're buying the same books on Amazon or something like that you're not too bothered about the adverts that are coming back from there, that's just the smart world we're live in. But if suddenly you lost all of your money from the account because of it haha, that would be the ultimate worry. If all your personal details get hacked. But you don't need to have a smart home for that now, do you. They can get your details from a hole in your wall where you put your card in. So that's, whatever you do you're at risk are you. Someone taking your details.

(I)
Yeah, so with the data then, that you are entering to the smart devices and that the smart devices are using. Do you see that they available for you, always when you need it [...]?

(U)
Yeah it is yeah. I can turn it on now and it will tell me, I can go back two weeks and see at what time of the day there was someone in my house. Yeah.

(I)
Yeah. Would you see there is any risks that that kind of data could be manipulated from anyone?

(U)
Well, yeah I think there it's probably available. So if I was a person whose' habits I was using, is I was going to work the same times by every day monday to friday and I'm the only one in the house at other times so they could be, that data could be built in to a bit of a record and a trap to say "well there is never anyone in that house between 9 and 5 monday to friday", that would be more of a worry yeah. But yeah that's based on someone using a, someone, sorry who's always in the house at the same time but I'm not. I think they would probably find my, 'cause I live and work quite close. I tend to be in and out at different times all the time. So I think someone to trying to find out when I'm definitely not gonna be there, wouldn't affect me as much. I would be more worry about it if I was living on my own and I just went up at 9 every morning and got home at 5 every night and someone could see that there was never any motion in the house at any other time. Because even if I don't set the detector up for the motion itself that still records it. So i don't, if I don't turn it on I don't get the text messages but I still, I still get it when I look at it I can still look back and see if there has been anyone in the house. Because I forgot to turn

the system on. It's too late then isn't it but you know what I mean it's still, that's still recording the data. So that's a little bit, again, but I'm not, that to me is the trade-off between having something I want and not. Yeah. But that's no different from on the central heating systems if people's heating system get switched on at a certain time. If they think that, that someone is buying in to a smart system of turning the heating off for when they're not in the house and turning it on when they're half an hour before they get home, they can record that data to see when you're switching it on and when it's getting switched off. As there, why would anyone not want it switched off on a cold day there is no one in the house. So if that was the same times every day, people could, what people think they have be trapped for. Then sort of like, almost like, not spied on but yeah, spied on is probably the best word isn't it. They can spy your movements by when your heating is not on. So that's another reason for why I probably would rather turn mine on and leave it on all day or turn it on low so they can't then tell it's not switched on but it's not on high so I don't, I don't leave that trace of when it's no one in the house by switching off the heating when I'm out. Probably otherwise, they can do that as well. You can probably find the same thing would happen on your internet use, wouldn't you?

(I)
Pardon?

(U)
You can still find that same information from your internet use, if your wifi is not being used for 8 hours a day, and all of the sudden at 5 o'clock the first thing you do when you come in is turn your laptop on. They could trap your movement, couldn't they, of the usage. You got the GPS on your phone haven't you.

(I)
Yeah.

(U)
Yeah, so when you're in the house on your own they can tell where you are by your phone probably haha.

(I)
Haha yeah true. And track you, as you say, with the, where you've been and then ask you to rate the cafe where you just went for a coffee or so.

(U)
Yeah exactly, yeah. So you, you go online and they ask you to give feedback on how good the service was in the cafe. And it's almost someone knows where you are. It's like you've got a

little buzzer. It's a little, it's a device out now which you can get to toddlers which you can strap on to the toddler, so if you're out with your little ones and you've gone out somewhere like a busy park or a shopping centre or something or a beach or anywhere really. You've got a wristband on the toddler and you've got on, you have an app on your phone so if that toddler wanders off and you can't see him, you can follow him on a tracker. It will buzz a signal at you so you can actually get a device for your kids just to let them wander off about 50 or 60 meters but you know where they are by a tracker haha, crazy isn't it? Yeah, that's what a mobile phone does isn't it?

(I)
Yeah exactly it is, yeah pretty much the same thing 'cause it's the GPS that you're carrying around anyway so.

(U)
Yeah, you're always being monitored.

(I)
Yeah. So with the smart device aswell, the permissions for you as a main user, like if you would put yourself as the owner basically, the admin, do you think that the permissions for other users on that system, do you think it is enough for you to set the right permissions for everyone or do you think there is any risk that the permissions could get mixed up?

(U)
Yeah it can, it can get mixed up. Yeah, I've been out somewhere and my device is telling me that I've got my central heating switched off. And that has nothing to do with me giving permission to somebody else. If I wanted [...] to have access to all my smart things, I think you can do that with a second phone. When I've been out away from home and I've looked to see if my motion detector is going off, and it has automatically switched over to tell me my smart heating system is switched on or whatever it was. Because it obviously picked up somebody else's' signal in the room or bar where I was at. So I must've picked up somebody else's information. I've no idea who it was, but it must have been someone in that same place. So I turned mine off and then turned it on, went outside and came back in again and it had gone. So that does get switched occasionally. Because I knew what happened 'cause it's sort of like, you know that's a bit like when the doorbell has gone off before. And its switching the case off, it's telling me my heating is on or off I can't remember what, but I haven't got the heating control so that can't know my heating is on or off. I haven't got a device connected to my heating. But, so that was obviously somebody's. But that wouldn't then let me get in to my system because that was picking up somebody else's. So I had to go outside and thought hopefully I would loose that signal and turn it off and turn it on and come back in again, and that was alright. But I haven't had that since, but

that must happen because it happened to me so I know it happens. So if that was the sort of thing that happened regularly and I was forever trying to set up my, it's not like fraud here, it's like you picking up somebody else's information aren't you?

(I)
Yeah, so how was your reaction from that?

(U)
Well I wasn't too impressed but that happened within probably a couple of days of me first getting it. So at first I'm thinking well what has happened, I wondered if maybe like I switched it on wrong. But you can't switch it on wrong you just press the button and that comes up, so you can't really do anything wrong but to tell you the heating is on, is like well, no it isn't that's not me. And I couldn't switch, I couldn't switch it from. Normally I could switch mine from light bulb mode to motion detector to sockets, so I can actually control on or off with the devices I've got. And you can even change, I forgot to, smart bulbs I can even say which is which room. One is the hall, two is the lounge etcetera. So I know to just change them over, they're all on the screen. You just press the button for the one you want, but this wouldn't let me swap anything over so whoever's device I was linked in to, he only had central heating. Because he didn't have any more buttons on there that I could even get confused with. So if he had a couple of bulbs, I would've probably been able to turn his light bulbs on haha. So at the time I was a little bit like, well that's weird that's not good. I thought the system had gone funny. For some reason that's not picking up the right thing that's telling me wrong. So I thought I will see if that happens again but that hasn't happened again and I realised that was picking up somebody else's device. That wasn't mine I was looking at. So that, yeah again, if that would've happened again I would've probably rang up the company and told them to cancel it. Because there is no point having a device which I'm paying for if you can't control it. Which is picking up everyone else's. But the worry is the more devices like that they sell, is that's gonna happen more frequently. And as long as they can't then find out who's control, yeah if that happened to mine, someone switched on my device without me knowing at the time and then later on I find out that that is what have happened, then it's time to say it's not worth having. But if there is only that many frequencies that are out there, I don't know how it work, but if them frequencies, you know in a time they will be all saturated. Yeah, that's the future thing, you know that hasn't happened since.

(I)
Yeah, I guess that's kind of disturbing though if somebody else is getting, or I mean that could happen to your information and somebody else got it.

(U)

Yeah, I don't know how many times somebody else has got my device on theirs. Probably never. Because to me quite honestly, when I go out I don't take notice, if I'm on the phone that's a bit like, unless with somebody that's where I get my text message pinging to tell me that has happend. I don't tend to look at it anymore. Now before I go out of the house, then I set the motion detector when I go out from the door. Because there is no point having the motion detector on while I'm in the house because that will send me a text message every five minutes. So it's still going off even if it's just someone walking about so I only set the motion detector when I'm out of the house. But that still uses, still controls the data, but the actual messages come back to, the text messages comes back to me when I set, unable it to control it. So when you're out of the house, set it up when I go out, I don't look at it until I get in. And I will do it before I walk through the door. When I sometimes forget or I come in and I get a text message within like 10 seconds of being in the front door. So then I think I might switch it off now. They're quite good though, they're quite handy. If you're living in a slightly dodgy area and you're a bit worried about forgetting to lock your door or something, they're quite good.

(I)
Yeah, like we said before, it's so many pros and cons with them so it's just all about bringing them together and see what you prefer from all the different devices that you want and what you think is worth using.

(U)
Yeah, if you're living in an area where the crime rate is going up and you think that can make your house more, more of a, it sounds horrible really but you know the idea is to send the burglars down your neighbor and not to yours haha. If you've gone to the trouble and buying you some, like a bit rottweiler dog and security cameras, then, so anyone potentially is gonna look at your house as a target but I think I will be safer than you next door without the dog without the burglar alarm or without the camera. So yeah alright, if I send someone next door rather than yours, make it targeted, well you've done your job haven't you haha. In a way, yeah. And that sounds nasty, that's up to them to protect their own property. And I will just see what I've got is more protection than the risk of what they put, they're giving away.

(I)
Ok. Well, I think I'm happy with the, everything I've got regarding this. It's really, yeah thank you so much, it's really really helpful with everything that you've said.

(U)
Ok good, thanks.

7.2.4 - Användare 4 (IPA4)

Datum: 2018-05-01, 19:29-20:07
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Då tänkte jag börja fråga vad din definition av personlig integritet är.

(U)
Till exempel när man är ute på internet. När man går in på olika sajter så är min syn på personlig integritet att man inte kan spåra mig tillbaka på vilka sajter jag varit ute på då. Men det kan man ju nu i för sig men man borde inte kunna det.

(I)
Rör det sig främst då om internet menar du då eller hur tänker du?

(U)
Ja främst internet då alltså. Ja.

(I)
Yes. Perfekt. Och då tänkte jag såhär att hur ställer du dig till att smarta enheter samlar in data om dig?

(U)
Nej det tycker jag inte är bra. Det tycker jag inte alls är bra.

(I)
Mm, varför då?

(U)

För att det är oftast privata företag som säljer information till andra privata företag eller myndigheter. Och det vill jag inte vara delaktig i. Ja.

(I)
Okej. Vet du vilken information som de smarta enheterna samlar in om dig?

(U)
Ja i hemmet. [...] Det är ju främst datorn då. Ja möjligen TV:n. TV:n kan ju det genom sin programvara i för sig. Eftersom vi har Netflix och sådant där. De programmen håller ju reda på vad man tittar på och allt va. Det gör de ju. Och även operatören.

(I)
Ja okej. Har ni försökt ta reda på exakt vilken information som samlas in från er?

(U)
Nej egentligen inte. Nej det kan vi inte säga att vi gjort. Man tittar ju på "history", jag menar "history" är ju gamla sökfiler. Och jag menar operatören har ju säkert, vet ju säkert var man har varit eftersom man brukar ju få ett mail ungefär tre sekunder efter man vart inne på någon hemsida. Med reklam ja.

(I)
Ja. Finns det någon orsak till att du inte har försökt ta reda på det? Vilken information som samlas in från dig?

(U)
Ja bekvämlighet antar jag.

(I)
Vad menar du då med bekvämlighet?

(U)
Ja att inte anstränga mig att göra det. Men däremot så försöker jag. Alltså egentligen försöker jag att inte använda sådana saker som att inte använda Google hela tiden utan växla lite grann va och så vidare faktiskt. Ja men de fungerar ju på samma sätt så de är ju oftast strunt samma. Men egentligen är det ju lite grann som protest för jag gillar inte att de där storföretagen använder oss som inkomstkällor. För det är ju det dem gör. Ja.

(I)

Tror du just med det där kring vilken data som samlas in, kring hur den hanteras och liknande, tror du att företagen försöker vara tydliga kring vilken data som samlas in och hanteras?

(U)
Nej. Det tror jag absolut inte utan de är ju bara intresserade av att sälja informationen vidare till annonsörerna. Det är ju det dem lever på. Att dem, försöker så att säga ta fram ens personlighet eller ja, och så sen sälja till rätt annonsörer. Det är ju hela affärsmodellen. Ja.

(I)
Tror du alltså då att företagen använder den insamlade datan främst för sitt eget syfte eller för dig som användare för att göra det så bekvämt då för dig som möjligt?

(U)
Ja det är väl både och egentligen. Men främst, de tjänar ju inga pengar på mig egentligen, utan de tjänar ju pengar på företagen som köper informationen av dem. Jag är ju bara en bricka haha.

(I)
Haha.

(U)
Så jag menar det är ju, produkten är ju att de ska sälja annonser. Alltså det är ju ett rent annonsföretag. Facebook och Google [...], det är ju det dem säljer. Men det är ju datorer. Men jag menar TV:n är ju kopplad till bredbandet så att det är ju ingen skillnad numera på en TV och på en dator så att säga.

(I)
Mm. Och om man kollar då på, jag frågade ju om du visste vilken information som samlas in.

(U)
Ja.

(I)
Vet du hur den här informationen sedan hanteras av företagen?

(U)
Nej det vet jag ju inte, jag bara, det ända är ju att man märker att de på något sätt har ju de här företagen som sen skickar reklammailen haha. de har ju fått reda på vilka sidor jag har varit inne på eller ungefär. Inte vilken sida, men vilka typer av sidor jag har varit inne på i alla fall va. Om man går in på någon resesajt och så, det dröjer ju inte länge innan man får reklam från flygbolag

eller hotell va. Och det får man ju inte annars, utan man får det ju i perioder när man vart inne på vissa sajter.

(I)
Och finns det någon orsak, där också, till varför du inte har valt att eller försökt att inte ta reda på det?

(U)
Nej jag antar att jag inte kan kanske haha.

(I)
Haha.

(U)
Jag har ingen lust haha. Jag har ingen lust. Jag menar jag är lite irriterad att det används på det sättet. Det är ju en sak. Men jag har ingen lust att forska vidare och ta reda på vilka företag som har fått vilken information utan jag bara märker att det är ju så det fungerar eftersom man får ju reklam från vissa företag. Beroende på vad man söker va. Så det är ju så det funkar. Och det är ju ingen hemlighet jag menar, det är ju så dem bygger affärsmodellen.

(I)
Mm. Om vi sen då kollar på just med att, okej de samlar in en viss data om dig. Och sedan, hur ser du då på kommunikationen som sker mellan enheterna? Till exempel att du, jag vet ju inte om du då kanske styr din smarta TV med mobilen också, att just kommunikationen mellan mobilen och TV:n då till exempel. Hur ser du kommunikationen mellan de enheterna där?

(U)
Ja vi använder ju, alltså man kan ju lägga upp databilden på TV:n så sätt. Men vi använder ju inte TV:n som en dator på så sätt det gör vi ju inte. Förutom ja, naturligtvis det finns ju appar man använder va. Men vi söker ju inte med Google eller med någon annan sökmotor med TV:n direkt, inte direkt. Det gör vi inte.

(I)
Okej. Men om vi då istället tänker på när information och data från dina smarta enheter till övriga system som till exempel företagens servrar, litar på du att den kommunikationen och överföringen sker på ett bra sätt?

(U)
Nej, eller vad menar du med på ett bra sätt?

(I)
På ett säkert sätt. Att liksom, informationen överförs säkert.

(U)
Nej alltså jag ser det som så att alla företag, haha, som är i den här branchen och som säljer saker och ting till oss, Apple eller vad det än är, är privata företag som tjänar pengar på att sälja information. Så jag litar inte på dem alltså det gör jag absolut inte. Men jag använder det eftersom jag tycker det är ett effektivt sätt att hitta informationen och kommunicera med andra människor och sådär men jag litar inte på det. På systemet, absolut inte.

(I)
Nej okej. Om man tänker att, just det här med att du har användarkonton till exempel på din smarta TV då. Och att TV:n även spårar vissa mönster från dig som användare, från saker du sitter och tittar på till exempel. Eller program som du sitter och kollar på.

(U)
Ja det gör den.

(I)
Och just den här typen av information, ditt användarnamn och lösenord och liknande, som då kan vara kopplat till vissa TV-program och så.[...] litar du på att överföringen av den typen av information är säker mellan företagens servrar, med all information som dem har från dig. Att överföringen mellan deras enheter och dina enheter är säker?

(U)
Nej det litar jag inte på.

(I)
Varför inte?

(U)
Därför att det verkar som att dem här, alltså det är ju hela tiden i medier att hackers kommer in överallt va. Och banker. Sedan om de nyheterna inte är korrekta det vet jag inte, men om de är korrekta så bevisar det ju att systemen inte är säkra. Inga system är ju säkra egentligen, det är de ju inte. Verkligen inte. Det är ju enda slutsatsen man kan ta tycker jag att är man någorlunda duktig så verkar det som man kan hacka sig in var som helst va.

(I)

Ja. Men använder du då ändå dina smarta enheter trots riskerna på grund av att ni anser att vinsten då är större än riskerna eller?

(U)
Nej egentligen är det ju att jag använder, man använder ju internetbanker eftersom det inte finns några vanliga banker längre haha. Så jag kan ju inte plocka, jag kan ju ställa mig ställa mig i banker i för sig. Det finns ett bankkontor kvar i Sverige, eller i [...] som, där man kan betala kontant. Men vissa banker de har ju inte ett enda kontor kvar som man kan betala kontant, räkningar va. Så vi är ju tvingade att gå ut på nätet och betala, det går ju inte i annat fall.

(I)
Ja, nej men precis. Och om man kollar då just i förhållande till din personliga integritet, och hushållets personliga integritet, när ni använder smarta enheter. Vilka ser du är de största riskerna när du använder dig av smarta enheter?

(U)
Nej det är väl när man håller på med pengar och betalar räkningar tycker jag. Det är alldeles för mycket nyheter om att det inte fungerar på ett säkert sätt den här gången. Sen att man haft turen att råka illa ut det är ju en sak men många har ju råkat illa ut och då är det ju ett elände för att reda ut de här. Och kreditkort det är ju samma sak, jag menar smart kort. Och det är ju absolut inte säkert. Det skimmas och så vidare. Känner ju själv folk som har blivit av med pengar. Och dem får ju inte, ibland får de ju inte ens tillbaka pengarna av bankerna. Så det är, jag menar systemet är inte säkert. Det är det ju inte, absolut inte. Och jag tycker det främst är det här banksystemet som är, borde vara betydligt bättre. Det ska ju vara helt omöjligt att kunna tränga in tycker man. Men det är det ju inte idag.

(I)
Haha nej, uppenbarligen inte nej.

(U)
Nej det är det ju inte.

(I)
Om vi tittar också på just på smarta enheter, det finns då områden att dela in de smarta enheterna i. Och det finns då fyra kategorier: energi, hälsa, säkerhet och underhållning[...][4]. I förhållande då till säkerhet för den personliga integriteten, vilket område för insamlad data anser du är mest känsligt?

[4] Begrepp förklaras för intervjuperson

(U)
Det är väl klart, hälsan är väl. Jag menar det beror väl på hur mycket man kan styra. Om den styr någon typ av dosering och det går fel där så är det ju klart att det inte är så bra. Eller ja hackar in som sagt. Men nej, ja hälsan. Och energin är väl inte så bra heller om det är någon som hackar in och sänker eller höjer temperaturen så mycket av någon anledning.

(I)
Mm, men om du skulle välja någon av dem i förhållande för säkerhet av den personliga integriteten. Vilken information är det då som är mest känslig?

(U)
Ja egentligen är det väl hälsan då. Om man kan styra doseringar och annat genom dator så blir det ja. Om någon annan går in i systemet då, det ju klart det är allvarligt.[...]Alltså egentligen, det som jag sa förut, jag menar även med det är ju även bankärenden och så vidare va, men hälsan då naturligtvis. Det är ju ganska viktiga saker ja.

(I)
Ja okej. Påverkar alla de här riskerna som vi har pratat om, påverkar det valet av de smarta enheterna som du väljer dig att använda dig av?

(U)
Ja på sätt och vis är det ju det. Alltså, jag är inte med i vissa sajter eller sådana här ja typ Facebook och så vidare. Och det är enda skälet till att jag inte. Jag är trött på att dem här företagen tjänar pengar haha. Ja och det finns alltså den här, för mig så räcker det med sms och mail och telefon. Ja, och sedan om det är säkrare det vet jag inte va men det är i alla fall inte den här systematiska insamlingen av information. Så där är jag inte med på grund av att jag är emot det. Och att jag ibland byter bort Google också för att dem… sedan är det ju kvitt samma i för sig men. Nu går jag i en liten protest tror jag haha.

(I)
Jaha haha.

(U)
Nej jag tycker det är fel att, jag tror det är något gammaldags det här med att internet ska vara fritt va, och det lever kvar fortfarande men det funkar ju inte längre när det är sådana enorma företag som ligger i bakgrunden va, och använder sig av internet. Det är ju helt annan sits nu än för 20 år sedan när det började. Det är inte samma sak längre.

(I)
Mm nej. Och om vi fortsätter spinna vidare på det lite, vet du vem som äger rätten till datan som samlas in från dina smarta enheter? [...]

(U)
Det beror väl på vad jag har använt för typ av mjukvara antar jag. Eller för typ av program. Jag menar använder jag Google så får den ju reda på precis var jag har varit och varför och så. Och då förutsätter jag att de äger den datan. Det står säkert i något, väldigt liten text någonstans. I kontraktet. Det tror jag alltså sökmotorn, så är det operatören där. Och sen, jag menar sen är det ju det att operatören som man använder, telefonföretaget dem används och får ju också information. Och jag menar de använder säkert också den informationen som de behöver så att säga, som de får in.

(I)
Mm, men är det någon information som du har försökt att ta reda på och hitta information omkring?

(U)
Nej. Nej det är det inte, det är alltså det enda beviset det är som jag sa att man får reklammail och ja.

(I)
Ja. Och finns det någon orsak till att du inte har försökt att ta reda på det?

(U)
Nej det är ju bekvämlighet haha. Nej att jag inte riktigt vet hur man ska söka efter den egentligen.

(I)
Ja, och om man kollar sedan också, du sa det att jag det är förmodligen den operatören.

(U)
Ja eller alltså man kan väl i för sig gå in på Google och så begära all information de har. Det har man väl rätt till vad jag förstår i för sig men ja. Men det har jag inte gjort. Jag tror att det stämmer men jag vet inte om det kanske, jag tror man kan göra det på Google också. Facebook kan man ju men ja.

(I)

Mm. Vet du sedan då vilka som har tillgång till den datan? Att visst, det sa du att du trodde att till exempel operatören då äger rätten till informationen och till exempel Facebook och Google. Men vet du vilka sen som har tillgång till den informationen då?

(U)
Nej jag tror inte att operatören har tillgång till Facebook och Google, utan det är ju då Facebook och Google. Men däremot så har väl operatören, operatören kan väl säkert också se vart, ja varit ute någonstans och gjort på nätet det tror jag nog. Men ja, alltså det är ju på något sätt är det ju såhär, ett problem tycker jag är att det är ju ingen myndighet som gör detta va, det tycker jag är ett stort problem. Utan det är privata företag och man har ingen insyn i de här privata företagen utan det är ungefär som att lite grann har det varit som att, jo men de håller på med internet så de är säkert jättesnälla och de hjälper till att agera. Och så litar man på dem och det finns ingen anledning att lita på dem egentligen va. Och helt plötsligt så kanske det inte sitter någon som är sådär jättesnäll i ledningen för dem och då… ja. Jag tycker det är väldigt, väldigt godtroget är det. Otroligt godtroget. Att man ger ifrån sig så mycket information helt frivilligt va, det tycker jag. Men jag har inte sökt, jag har inte tagit reda på vad de har egentligen det har jag inte.

(I)
Mm okej, nu ska vi se. Om man kollar då sedan på det här med att ja, din smarta TV då. Litar du på att dina smarta enheters system funkar som de ska? Att de lagrar saker som de ska och ger dig den informationen som du ska ha och så?

(U)
Ja alltså det verkar den ju göra haha.

(I)
Haha ja.

(U)
Alltså jag menar rent tekniskt funkar det ju, det gör det ju. Det är ju inga problem så sätt.

(I)
Anser du att det finns någon risk med att datan som din smarta enhet innehåller kan bli manipulerad?

(U)
Ja det kan den väl naturligtvis bli. Jag menar det håller man ju på att prata om hela tiden att man kan, ja lägga ut falska nyheter och ja, hjälpa fel typ av människor att vinna val och annat. Ja.

(I)
Ja okej. Är det något som du ser som ett problem eller är det något som du ser att du inte bryr dig om riktigt?

(U)
Nej det är ju jättestort problem det är ju klart. Nej men enkelt man kan ju säga såhär, summan av kardemumman är ju att jag tror att man måste kunna, man måste börja att reglera internet man kan inte låta det vara fritt längre. Det går inte alltså. Det är alldeles för många som har egna syften som manipulerar internet. Ja nej men det är väl, jag tror det hänger ihop med att i början så var det, alla tyckte det var fantastiskt för 20 år sedan då. [...] Det enda som skulle vara fritt här i världen det var internet så att säga, och det hänger kvar va. Och nu finns det sådana som utnyttjar det va. Jag menar det är ju dagligen så ser man ju att det, att internet utnyttjas. Och det måste man, för att skydda då, vad ska man kalla, vanliga medborgare som inte är ute i ja... jag tror man måste på något sätt reglera det. Faktiskt. För att skydda viss information. Det tror jag.

(I)
Ja. Men just med information på enheter. Anser du att din data som du har där i, ja den data som du har i din enhet. Anser du att den är tillgänglig för dig hela tiden när du använder den?

(U)
Ja, det är den ju. Jo rent tekniskt fungerar det ju fantastiskt va. Om det är det du menar.

(I)
Ja.

(U)
Men det är ju just den här manipuleringen som [...] som är väldigt aktuell i och med att man pratar om det, det är väl bevisat mer eller mindre att man har, man kommer ut med falska nyheter man använder internet på ett nytt sätt va. Ja, och det är ju klart det är ju inte bra, det är ju farligt.

(I)
Ja men det har också lite med spåret att göra det här med manipulering av data. Din enhet eller de enheter som du använder dig av. Anser du att de har tillräckligt med begränsningar för olika behörigheter? Till exempel att du som admin har ett särskilt kodlås av enheten för att begränsa andras behörigheter?

(U)
Jag tror väl att man kan försvåra såklart men jag tror ju att det finns sådana som är tillräckligt duktiga att kan gå igenom allas behörigheter om det nu skulle vilja det. Ja det tror jag. Och jag

menar de använder ju vissa sätt som, i vissa appar finns det ju olika ja haha. Appar har stoppat in vissa saker i apparna som ligger och lurar i bakgrunden. Sedan om det är sant det vet jag ju inte men jag menar det kan jag ju mycket väl föreställa mig. Ja nä så det är ingen, jag upplever det som att det är en väldigt bekväm, man använder, det är en väldigt bekväm teknik men man kan inte lita på den va. Nej det kan man inte. Nej absolut inte. [...] Man kan ju säga såhär att en dator är ju jättebra så länge den funkar. Men en dator funkar inte hela tiden. Helt plötsligt så bara, den slutar fungera. Och då är den ju inte så att säga, alltså hela hemmet hänger på datateknik och den typen av teknik för det fungerar aldrig hela tiden. Det är alldeles för sårbart va. Alldeles för sårbart. Jag menar igår hade vi lite problem med bredbandet här, hade kylskåpet hängt ihop med bredbandet så hade vi väl fått slänga mat i morse ungefär va. Jag menar det funkar inte, det är inte tillförlitligt rent tekniskt. Inte än då. Det är det inte.

(I)
Mm. Men säg då om, även din TV där, att den eventuellt tar upp data från dina gäster, eller samlar in information. Vad tycker du om det?

(U)
Nej jag tycker det är förkastligt att apparaterna samlar in information om oss, och vi är inte medvetna om det kanske. Det var inte därför jag köpte TV:n haha.

(I)
Nej haha.

(U)
Haha, nej faktiskt inte haha. Nej men ja, jag tycker inte om det. Såklart.

(I)
Nej okej. Men vilken är den främsta orsaken om vi säger så, till att du införskaffade dig smarta enheter?

(U)
[...] Jag tycker man blir alldeles för sårbar. Det första så kan strömmen gå va, det händer ju faktiskt fortfarande i samhället. Och då har du ingenting plötsligt. Och nu har vi ju bredbandstelefoni också, förut hade vi ju bredband med en vanlig telefon. Och få var det ju faktiskt så, då hade man faktiskt, när hela mobilnätet låg nere och bredbandet, så kunde man ju faktiskt fortfarande ringa. Ja, men det kan man ju inte längre idag. Så samhället blir ju alldeles för sårbart va. Alldeles för sårbart. Och jag menar, jag tror att samhället är, jag tror att människor som bestämmer, myndigheter och politiker, verkar lita väldigt mycket på datateknik. Vilket är skrämmande tycker jag. För det är ju, det funkar ju inte annars, det är ju så enkelt va.

(I)
Mm men precis. Och vad är största orsaken till att du har valt att ändå använda dig av smarta enheter då?

(U)
Därför att man, därför att utveckling har drivits så långt så att man klarar sig inte utan va. För att göra ärenden och ja för alla jag menar, alla myndigheter och allting de har ju sina digitala mailboxar och så vidare. Om inte annat så lägger de ju, varje räkning kostar 50 kronor extra om man inte använder digitala räkningar för det är elräkningar då. Jag menar de tvingar ju en att använda datorer, systemet tvingar ju en att, det finns inget alternativ.

(I)
Aa. Och om i hemmet då? Till exempel TV:n då, vad är orsaken då till att man väljer, eller till att du väljer att skaffa en smart TV istället för en vanlig TV?

(U)
Nej det finns inga dumma TV:s längre haha.

(I)
Haha.

(U)
Alla TV-apparater är ju smarta haha.

(I)
Haha, ja kanske det haha.

(U)
Jag menar jag såg inte en enda dum TV där i, haha, i affären. Nej men det finns ju bara den här TV längre, den är ju, jag vet inte om det säljs någonting annat längre. Jag tror inte det. Man kunde ju ha behållit sin gamla analoga tjock-TV.

(I)
Ja den är ju inte helt fel den heller haha.

(U)
Nej alltså man ska ju inte överdriva, men jag menar, jag tycker att man måste tänka [...]. Jag upplever det som att man är väldigt naiv då. Man litar för mycket på data, ja teknik. Och jag tror

jag är extra, ja du vet ju vad mitt yrke var så att säga va, så jag är ju så att säga hela mitt yrkesliv varit utsatt för datorer och speciellt har jag varit utsatt för när de inte funkar. Ja, och systemet är då så att säga till 100% konstruerat för att allting måste fungera. Och så gör det inte det ändå, ja då blir man väldigt utsatt så att säga. Och det är ju väldigt, det är ju hela samhället att man, att man bygger upp allting kring den här tekniken och så finns det inga backup-system va. Det är ju det som är problemet. Ja. Man håller ju till och med att ta bort pengar så att säga så att när nätbankerna inte funkar längre så säga av någon anledning så kan vi inte ens längre gå ut och köpa mat. Alltså det är ju, det är inge, man kan säga såhär det är ju inget bra system haha. Och Sverige, jag reagerar på det att Sverige är ju extrema när det gäller den här utvecklingen. I de flesta andra länder så vägrar man att gå så långt som vi har gjort. I Tyskland, jag menar, det är ju till och med i vissa affärer vägrar de ju att ta kort fortfarande nästan. Eller de tar bara vissa kort. Och här är man ju konstig om man inte swishar fram och tillbaka överallt. Så jag menar jag tycker tyskarna har en bättre inställning faktiskt. Lite mer realistiskt.

(I)
Ja men okej. Yes, men jag är jättenöjd över de svar jag har fått från dig och dina tankar och åsikter kring det här. Så jag får tacka så jättemycket. Tusen tack för din hjälp.

(U)
Ja tack själv.

7.2.5 - Användare 5 (IPA5)

Datum: 2018-05-05, 12:12-12:39
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Vad är din definition av personlig integritet?

(U)
Den data som angår bara mig, det kan vara personliga uppgifter. Alla uppgifter som finns på nätet, som har hamnat där utan mitt godkännande.

(I)
Hur ställer du dig till att de smarta enheterna samlar in data om dig?

(U)
Om de samlar in data om mig som är tillgänglig endast för mig då är det okej, men om de samlar in data som obehöriga kan få tillgång till då tycker jag inte att det är okej.

(I)
Har du tittat upp vilken information som de smarta enheterna samlar från dig?

(U)
Det går typ inte, eftersom det är så pass omfattande. Till exempel Google, de använder sig utav variabler som man själv inte förstår och då tar det flera timmar att sätta sig in i det och sen tar det ytterligare flera timmar att förstå konsekvenserna senare. Jag har försökt, sen har jag stängt av en hel del inställningar. För när jag har kollat igenom det, så är det totalt onödigt. De flesta leverantörerna till smarta enheter, de kräver foton osv.

(I)
Anser du annars att informationen är lättillgänglig för att hitta det?

(U)
Den är inte lättillgänglig, man får anstränga sig för att hitta den.

(I)
Vad är din åsikt kring att de samlar in den typen av data?

(U)
Min åsikt är att, många gånger... Krav på tillgång till enhetens funktioner, har jag svårt att förstå varför de ska ha tillgång till den informationen, och sen vet man inte hur den används sen.
Jag gillar inte att det.

(I)
Hur ser du på kommunikationen som sker mellan enheterna? Pålitlig? Riskfylld?

(U)
Jag förstår att sådan kommunikation måste ske för att saker och ting ska fungera. Men sånt kan missbrukas av någon. Ja jag uppfattar att det finns flera risker med kommunikation. Till exempel moln, det har hänt att folk har fått tillgång till någon annans bilder av någon form av misstag.

(I)
Litar du på att den insamlade data överförs på ett säkert sätt mellan de smarta enheterna du använder och övriga system som hanterar dess data, exempelvis företagens servrar? Varför? Varför inte?

(U)
Brister finns alltid I den här formen av kommunikationen. Så jag tror inte att, definitivt hundra procent säkert det tror jag inte

(I)
Vet du hur den insamlade data hanteras av företagen? Dvs, vad som händer med data efter att den samlats in av företagen?

(U)
Det vet jag inte. Oftast har man inte tillgång till den info om hur den behandlas, eller så finns det enkla termer som inte säger så mycket. Till exempel Facebook och Cambridge analytica,

(I)
Har du försökt ta reda på det?

(U)
Ja jag har försökt att göra det, och då tyckte jag att det var svårt att få fram. Informationen var utspridd på olika sidor från samma företag. Om man använder deras sökfunktioner på deras hemsidor så är de inte heller användarvänliga.

(I)
Vad är din åsikt om företagets/företagens sätt att hantera den data de samlar in från dig genom de smarta enheterna?

(U)
Jag tycker inte om det.

(I)
Vet du vilka som har tillgång till den insamlade datan?

(U)
Inte exakt nej..

(I)
Har du funderat på hur den insamlade data kan påverka den personliga integriteten i framtiden? Hur?

(U)
För det första, så är det ju, företagets syfte att tjäna pengar. Och då överskuggar det allt annat. Just den insamlade data kan säljas vidare och används av en tredje part. Så att jag tycker det är riskfyl

(I)
Vet du vem som äger rätten till den data som samlats in av de smarta enheterna?

(U)
I dagens läge, så finns det så många leverantörer att man inte längre förstår vem som äger vad osv.

(I)
Vilken är den främsta orsaken till att du införskaffade dig smarta enheter?

(U)
Egentligen så vill man ha tillgång till den nyttan de kan göra. Så det är nödvändigt ont att just ansluta dem och att de får tillgång till alla andra uppgifter kring mig.

(I)
Tror du företagen försöker vara tydliga kring vilken data som samlas in och hanteras? Varför? Varför inte?

(U)
Av min erfarenhet så är det inte speciellt tydliga.

(I)
Varför?

(U)

Oftast ger de inte motivering till varför de ska ha tillgång till mina uppgifter i tex mobilen, bilder osv. Företagen vill skydda sig själv och vill lämna så lite information som möjligt om varför de vill ha denna informationen.

(I)
Tror du att företag använder den data som samlas in från ditt hushåll, främst för sitt eget syfte eller för dig som användare?

(U)
Ja det är, lite svårt att gå in på det här också utan att vara kortfattat. Det är ju det här att visst, jag tror att jag har möjlighet eller jag har inte möjligt att påverka utan jag har möjlighet att tacka nej till vissa delar av krav till tillgång till enhetens diverse konton. Och då kanske jag inte kan använda deras funktioner eller så-

(I)
Ser du några risker för hushållets personliga integritet vid användning av smarta enheter?
Om JA:

(I)
Vilka anser du vara de största riskerna?

(U)
Ja det tror jag. Den insamlade data hamnar någonstans man vet inte var egentligen. Det finns ju risk att någon kan hacka in sig

(I)
Vilket område för insamlade data, anser du är mest känsligt i förhållande till den personliga integriteten? Underhållning, Hälsa, Säkerhet eller Energi? Varför?

(U)
Om man tar till exempel med Netflix, jag tkr inte om att de kollar på vad jag tittar och sen ska ge förslag på vad jag ska titta. Egentligen är alla områden kopplade till den personliga integriteten känsliga, men jag väljer säkerheten.

(I)
Påverkar dessa risker valet av vilka smarta enheter ni använder er av?

(U)
Jag var tvungen att installera en kamera som var uppkopplad mot nätet. Nej jag har inte slutat använda just den enheten.

(I)
Använder ni smarta enheter, trots riskerna, på grund av att ni anser att ”vinsten” är större än riskerna?

(U)
Ja det förekommer.

(I)
Vad tycker du om olika begränsningar och behörigheter i system? Till exempel i kodlås?

(U)
Jag ser det som ett riskmoment. Mina admin-lösenord osv, så försöker jag skydda det. Men i och med att det lagras på elektroniskt sätt, så kan någon få tillgång till det utan att man märker det.

(I)
Litar du på att enheternas system fungerar som de ska?

(U)
Av erfarenhet vet jag att enheter kan krångla.

(I)
Anser du att det finns risker med att din data kan bli manipulerad?
Om ja, Ser du det som ett problem?

(U)
Jag snarare anser att den data kan bli använt till något annat än den syftet som den hade från första början.

(I)
ser du det som ett problem?

(U)
Ja det är klart att jag ser det som ett eventuellt problem

(I)
Anser du att din data är alltid tillgänglig för dig när du behöver den?

(U)
För det mesta ja.

7.2.6 - Användare 6 (IPA6)

Datum: 2018-05-05, 12:12-12:28
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Ja jag tänkte väl börja med att fråga vad din definition av personlig integritet är?

(U)
Jag kan väl tänka mig att det är inget härleds till vem jag är samt att inget spelas in samtidigt utan mitt godkännande. Utan alltså jag måste ju veta det. Även min telefon, om den nu tar en bild på mig utan mitt godkännande, det blir liksom lite läskigt. Och om du tar ett foto på mig och lägger ut det på ett okänt forum, där kanske ingen vet vem jag är, det kopplas inte till mitt namn eller någonting, det är ju ganska, det är ju inte så farligt. Men så fort det står mitt namn eller bostad eller vad vem jag är, så är det inte okej längre.

(I)
Mm okej, men om jag då frågar om hur du ställer dig till att de smarta enheterna samlar in data om dig?

(U)
Är jag säker på att den data stannar inom ramarna där de ska, alltså för mina godkända mottagare, men det är liksom inte okej att mitt smarta kylskåp skulle dela med sig av min data till en tredje part för att marknadsföra reklam, då är det inte okej.

(I)
Mm okej, har du då tittat upp vilken information som de smarta enheterna samlar från dig?

(U)
Nej.

(I)
Okej. Finns det någon anledning till varför du inte har tagit reda på det?

(U)

Jag tycker att det är för mycket bla bla och svårtydda bla bla i texterna. Jag förstår att de måste ha ett språk för att täcka igen sina kryphål. Samtidigt där lagarna är tydliga, så är de liksom ändå är duktiga på att kunna få oss kunder att inte orka läsa texten och får oss bara jaja jag godkänner, utan att läsa igenom det dära. Även om informationen är lättillgänglig som är den inte alltid lättförstådd.

(I)
Mm okej. Okej men, har du försökt ta reda på vilken data de samlar in om dig?

(U)
Ja skummat igenom ibland för att få en överblick. Och där har man har ju sett att där står tredje part, men vad är en tredje part undrar man då? Och där tappar man en läsare eftersom man inte förstår samt inte orkar gå vidare och leta efter liksom, utan man bara accepterar det för att jag vill ha min grej nu. Jag vill inte att det ska hålla på en timme innan jag får den.
Och sen tänker man om flera använder sig utav den, då inte kan det ju inte vara så farligt för att flera användare också har godkänt den.

(I)
Anser du att informationen som fanns tillgänglig, för vilken data som samlas in, var tillräcklig? Varför/Varför inte?

(U)
Nej eftersom de använder termer som man inte riktigt förstår.

(I)
Om vi då tittat på kommunikationen som sker mellan de olika enheterna? Anser du det kan vara Pålitlig kommunikation eller att den kan vara riskfylld?

(U)
Åhh det är lite läskigt. Jag är inte utbildad inom säkerhet, och förstår inte allt det dära och tycker absolut att det är läskigt eftersom att jag inte vet vem som ser denna informationen som de samlar in. Och jag tycker också det är läskigt att dessa enheterna kan kommunicera och dela data om mig, någonstans jag inte vet var.

(I)
Mm ja. Litar du på att den insamlade data överförs på ett säkert sätt mellan de olika smarta enheterna du använder och övriga system som hanterar dess data, exempelvis företagens servrar? Varför/Varför inte isfall?

(U)
Nej eftersom att jag inte har 100 procentig egen kontroll över detta, så därför litar jag inte på det till hundra procent. Ser jag inte det, så finns det alltid en risk att någonting annat kan hända med det. Det är någonting som man får ta [...].

(I)

Vet du hur den insamlade data hanteras av företagen? Dvs, vad som händer med data efter att den samlats in av företaget?

(U)
Nej.

(I)
Okej. Finns det någon orsak till varför du inte har tagit reda på det?

(U)
Har inte orkat men jag använder ändå mina smarta enheter just för att göra det lättare för mig och min sambo är väldigt intresserad av sånt, så det är han som har köpt alla grejor.

(i)
Okej. Så du har alltså inte försökt ta reda på det?

(U)
Nej

(I)
Men till exempel anser du att informationen som fanns tillgänglig, för hur den hanteras, var tillräcklig?

(U)
Jag tycker, den är ju lite svårtolkad och egentligen vet jag inte vad jag kan lita på i den texten.

(I)
Aha okej. Men vad är din åsikt om företagets sätt att hantera den data de samlar in från dig genom de smarta enheterna?

(U)
Ja eftersom jag inte arbetar i deras mörkaste rum i deras kontor så har jag ingen inblick i hur de hanterar sådana saker, så kan jag därför inte kommentera vad jag tycker om det.

(I)
Ja, men vet du hur den insamlade data lagras av företagen?

(U)
Nej.

(I)
Okej, finns det någon orsak till varför du inte har tagit reda på det?

(U)
Jag är inte kunnig inom sådant, därför har jag inte gjort det heller.

(I)
Nej okej, så du har alltså inte försökt ta reda på det?

(U)
Nej, det får jag väl erkänna.

(I)
Okej, men om vi nu tänker på behörigheter till till exempel en kamera i smarta hemmet. Tycker du då till exempel att behörigheter är tillräckliga eller inte tillräckliga? Och om då en annan användare i hushållet får tillgång till din data och kan ändra den utan ditt godkännande, så att systemet inte känner av att det är en användare eller att systemet inte har loggat ut dig från enheterna. Tror du att det kan finnas en risk med det?

(U)
Ja absolut. Det finns smarta hackers som kan hämta den informationen hur lätt som helst om de bara vill och givetvis beroende på vilken enhet såklart men så länge jag som huvudanvändare eller vad det heter och kan styra och hantera ändringar, så vill jag kunna godkänna att andra än jag gör det. Men om andra människor i mitt hushåll får behörigheter är det en annan sak, men jag vill kunna se dem och absolut du kan hitta en hackare som hackar sig in och gör saker utan att jag märker det.

(I)
Mm, men skulle du säga att du som huvudadmin skulle då kanske vilja ha en större inflytande på dina egna smarta enheter och se kanske vem det är som, om det till exempel skulle loggas information eller om det är någon som är inne i enheten eller om det är någon som har använt sig utav enheten innan. Och sånt.

(U)
Absolut, det är bara tillräckligt bra att kunna och lära mig det, så hade jag absolut velat

(I)
Okej Men om vi då går till äganderätt av den data som samlats in av de smarta enheterna Vet du vem som äger rätten?
(U)
Nej, inte rakt upp och nej.

(I)
Nej okej. Men finns det någon orsak till varför du inte tagit reda på det?

(U)
Jag är väl lite lat. Jag antar att de som har gjort min enhet [...]. Det är så kallat deras data.

(I)
Eller vet du vilka som har tillgång till den insamlade data?

(U)
Nej egentligen inte.

(I)
Mm okej. Men om jag då frågar Vilken är din främsta orsak till att du införskaffade dig dessa smarta enheter?

(U)
Då är det ju min sambo övertalade mig. Han gillar teknik och det underlättar det en del i vardagen samt om det blir inbrott så kan man se vem eller spela in. Telefonen är ju givetvis mitt egna val men resten är hans.

(I)
Ah okej. Men tror du företagen försöker vara tydliga kring vilken data som samlas in och hanteras? Varför/Varför inte?

(U)
Lite tror jag att de försöker. Jag tror att de försöker sammanfatta sina regler småordigt eller fåordigt då och därför kan det sakna en del tydlig information för dem som inte riktigt förstår språket. Och många företag försöker hitta sina kryphål. Täcker för och öppna för dem. Och inte alla absolut inte, men det är många som, jag tror de som är ärliga och 100 procent verkligen är på kundens sida försvinner tyvärr in i mängden.

(I)
Okej. Yes men tror du att företag använder den data som samlas in från ditt hushåll, främst för sitt eget syfte eller för dig som användare?

(U)
Jag tror att det är lite både och, man gör inget som inte gynnar sig själv. De vill kunna behålla sina kunder och ha många kunder. De vill också se till så att de får en stor del av kakan. Så jag tror att det är på både hållen där. De vill på ett sätt veta så mycket som möjligt om sina kunder.

(I)
Mm okej. Då ska vi se. Ser du några risker för hushållets personliga integritet vid användning av smarta enheter?

(U)
Ja.

(I)
Okej men Vilka anser du vara de största riskerna då?

(U)

De är väl att företagen kanske använder mina uppgifter för andra ändamål än vad min enhet är tillför, eller då såklart att min kära hackare går in och tittar på mig eller ser och säljer min data eller någonting sånt där.

(I)
Okej. Smarta enheter kan delas in i fyra områden: energi, hälsa, säkerhet eller underhållning [...][5] . Vilket område för insamlade data, anser du är mest känsligt i förhållande till den personliga integriteten? Varför?

(U)
Ja alltså om de registrerar vad jag tittar på min tv. Det är inte ett så stort problem. Men registrerar de som till exempel vad mitt blodtryck är, eller varför de skulle göra det eller om jag har temperaturreglering, det är inte ett större problem. Det är fine. Men om någon skulle titta på mig i min kamera när jag pillar mig i näsan, är väl lite över. Och sen lite hur hanteras uppgifterna igen. Det är ju säkerheten som är den främsta. Jag vill ju inte att de ska titta på mig när jag petar mig i näsan, om de inte skulle betala för det haha.

(I)
Okej. Påverkar dessa risker valet av vilka smarta enheter ni använder er av?

(U)
Nej inte jättemycket just idag

(I)
Nej okej. Men är det så att ni använder er utav de smarta enheterna trots riskerna, på grund av att ni anser att ”vinsten” eller nyttan är större än riskerna?

(U)
Ja det gör vi

(I)
Okej. Anser du att enheterna har tillräckligt med begränsningar för olika behörigheter?
Tex. Om du har Kodlås; eller din kamera som du är admin ägare för, ja alltså för enheterna för att kunna begränsa andra behörigheter.

(U)
Ja men samtidigt nej eftersom allting kan hackas.

(I)
Ja okej. Men till exempel det här med för andra kanske människor som skulle kunna komma hem till dig. Tycker du att behörigheterna för dem är tillräckliga eller inte?

(U)

[5] Begrepp förklaras för intervjuperson

Det beror lite på. Jag har ju kylskåp, kamera och en telefon, vill de låna dem så ja, då kan de få låna min telefon men då låser jag upp den till dem.

(I)
Jo men det är lite det jag menar. Alltså just det här med låset, om det är tillräckligt.

(U)
Hade jag haft ett kodlås till min dörr, där jag hade vetat att någon man känner har också. Det tycker jag är lite läskigt, men visst kan man få en engångskod eller någonting, så kanske det är lite lättare att släppa in dem eller så kan de bara ringa på klockan som normala människor så kommer jag.

(I)
Okej Men sen om vi går vidare till integritet. Litar du på att enheternas system fungerar som de ska?

(U)
Ja ja måste lita på det eftersom att jag ändå använder mig utav dem [...].

(I)
Anser du att det finns risker med att din data kan bli manipulerad?

(U)
Ja

(I)
Okej men ser du det som ett problem?

(U)
Ja risken finns ju alltid. Det kan vara någon som har hackat den, bara för att någon tycker det är kul eller för att de kan, eller att den kan vara fel programmerat från första tiden. Många produkter är programmerade på det sättet att, och jag tror på det, att de går sönder i förtid.

(I)
mm. Och sen då sista frågan Anser du att din data är alltid tillgänglig för dig när du behöver den?

(U)
Ja, när jag använder dem så är det de i alla fall, som jag har uppfattat det som.

(I)
Mm Okej.

7.2.7 - Användare 7 (IPA7)

Datum: 2018-05-04, 11:39-12:06
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Vad är din definition av personlig integritet?

(U)
Jag skulle säga att det är den information som sprids om mig själv, eller finns om mig själv, att man var medvillig till att sprida den informationen. Alltså att man vet typ ungefär vilken information om mig själv som man ger vidare till andra aktörer eller människor liksom. Att viss typ av information som är personuppgifter som du inte vill ska komma ut eller vissa beteenden och så vidare, och ingen har rätt att ta dem utan ditt medgivande. Skulle jag säga.

(I)
Toppen. Och om vi fortsätter då med personlig integritet i bakgrunden på det hela. Hur ställer du dig till att de smarta enheterna som du använder dig av samlar in data om dig?

(U)
Jag skulle väl säga att jag är mer positiv till det än många andra. Av anledning till att jag tycker det är rimligt att viss typ av aktivitet som man gör på internet eller gör någon annanstans är väldigt öppen och borde samlas in. Man accepterar väldigt många olika typer av villkor, den typen av policys. Man accepterar kakor när man köper saker på internet eller är inne på olika typer av hemsidor. Så jag är inte så rädd att till exempel Facebook som visar information kring en, att "Oj jag har precis Googlat kring en potatis och nu vill de sälja potatis till mig på Facebook" och så vidare. Jag är inte så rädd kring det. Dock så tycker jag att information som samlas in om en, som man inte är tydligt medveten om att den samlas in, den tycker jag liksom inte riktigt är okej. Till exempel om det skulle vara åsiktsregistrering eller om det skulle vara var man befinner sig och den typen. För det är information som kan potentiellt hamna i andra

människors händer, för det är ju inte säkert de kan garantera säkerhet av den informationen. Och det är då man kanske måste ta, alltså de verkligen måste ligga på ansvaret att någon kriminell människa till exempel inte vet var jag ställer min bil eller var jag handlar eller var jag gör detta. För det kan vara en säkerhetsrisk. Så uppfattar jag det.

(I)
Yes. Har du kollat upp vilken information som de smarta enheterna samlar in om dig?

(U)
Nej det har jag inte gjort. Alltså man vet ju vilken information som presenteras om en ytligt på internet i form av reklam och så vidare. Och jag vet ju lite om hur kakor fungerar, så jag förstår varför de är där. Och liksom anledningen till det. Sen all information som samlas i olika typer av databaser eller säljs omkring, det har jag ingen aning om.

(I)
Mm. Finns det någon orsak till varför du valt att inte ta reda på vilken information som samlas in?

(U)
Jag har inte tid liksom. Jag har bara inte tänkt på det [...]. Jag kan tänka mig såhär att det är väl typiskt en sådan grej som du kommer agera på när det väl blir någonting obehagligt. När du väl märker "Oj, det här händer mig" eller någon har den här typen av information, är då man kollar upp det. Men så länge det inte händer någonting, så är det väl lite någonting att utgå från att nej men det är ganska lugnt liksom.

(I)
Mm. Tror du då att företagen försöker vara tydliga för dig som användare, med vilken information som samlas in?

(U)
Alltså jag tror att företag gillar att säga att de är väldigt tydliga för att ge förtroende och sådär. Beror på vad det är alltså, nej. Jag tror att det finns ett visst intresse, kanske politiska intressen som står emot individens egna intressen. Och det är väl dem, gör mig så långa agreement policys eller vad som helst som möjligt för att man själv inte riktigt kan medveten för annars hade man ju kanske varit medveten. De hade kunnat simplifiera texterna eller betydelsen av det som skickas ut till användaren mycket mycket tydligare. Men det gör dem inte. Alltså det är ju såhär om du tittar på vägskyltar eller någonting i trafiken så har de ju symboler och allting för att du enkelt ska kunna snappa upp exakt vad allting menas med. Men den typen av grejer använder man ju inte på internet. [...] Jag kan tänka mig såhär, reglering och sånt sätter vissa krav på att de

måste visa upp informationen. Men de vill gärna att den ska bypassas så snabbt som möjligt. Jag har själv, jag vet ju inte exakt vad de tänker. Men jag tror att det finns en, det finns lite intressekonflikt. Så nej, jag tror inte de är helt tydliga med vad de samlar in liksom.

(I)
Yes. Och du sa att du inte vet helt vilken data då som samlas in, vet du sedan hur datan vidare hanteras när den väl är insamlad av företagen?

(U)
Nej alltså man vet väl någonstans att det är klart, skulle man fråga väldigt mycket om till exempel resor till Turkiet eller vad som helst vad man kan göra, till typ Alexa kan du fråga hur ser säkerhetsnivån ut i Turkiet och så vidare, så kan de ranka det. Så man kan tänka att det kan vara kommersiella intressen som den samlar in. Alltså, vem vill rikta reklam eller alternativt marknadsanalyser och den typen av data samlas in. Kan jag tänka mig hanteras. Sen har jag ingen aning om det är politiska intressen eller underrättelsetjänst [...], vilken typ av marknadsanalys de gör och så vidare. De detaljerna har vi inte över huvud taget liksom. Men det är bara det man antar, för man vet ju inte hur dem hanterar data under lag och det är väl också någonting som är problemet[...]. I och med att deras tjänster är väldigt användbara, så får de ju godkännande av användarna hela hela tiden. Så på något sätt, användarna godkänner detta själva även fastän de inte vet vad informationen hanteras. Så att så kan det vara tror jag.

(I)
Mm och om vi då tittar på, du använder Alexa sa du?

(U)
Mm delvis.

(I)
Och då använder du flera enheter då som kommunicerar med varandra. Hur ser du då på kommunikationen som sker mellan de enheterna? Litar du på den?

(U)
Alltså just när det kommer till liksom kommunikation mellan Alexa och vår strömbrytare till exempel, och att hantera olika när det ska vara ljust och inte och så vidare. Den typen av styrsystem eller vad det är, ser jag inte så mycket problem med. Sen det är klart att den har ju även tillgång till min Spotify lista och så vidare. När jag bara säger “spela the Beatles” till exempel så sätter den igång the Beatles så jag kan lyssna på det. Och där vill jag ändå säga att

jag har ju liksom ett inlogg där och jag har ju ingen aning om hur den samlar in informationen om hur jag använder de grejerna liksom. Så nej, det skulle jag inte vilja säga att jag litar 100%. För den kan ju hämta information från det när som helst. Jag menar om den kan få tillgång bara genom min röst så kan den få tillgång annars också. Men just när det kommer till såhär funktionella grejer, typ som att "sänk ljuset i köket" till exempel. Så då ser jag inte så mycket problem med det. Utan det är mer om den får tillgång till konton eller olika användargrejer som vi använder.

(I)
Okej. Och litar du på att datan överförs från dina enheter till andra system, som till exempel företagens servrar? Just den kommunikationen av data mellan där?

(U)
Nej alltså jag har ju ingen aning hur det ser ut, så nej. Nej jag skulle inte säga att jag litar på det 100% än, och jag ser det väldigt mycket som en politisk fråga. För att följa på nyheterna liksom, de pratar om Amazon, de pratar om Facebook och om hur de hanterar alltihopa [...]. Och när de var typ i kongressen och de blev utrågade och grejer liksom. Om jag litar på det eller inte, det är väl liksom att jag litar på att det finns myndigheter, regelverk och lagar som hanterar detta till mig. Förhoppningsvis. Men jag litar inte riktigt på myndigheter och deras kompetens kring IT och informationssystem och styrsystem och alltihopa. Och det är väl lite där de brister liksom.

(I)
Yes, har du funderat på hur just den här insamlade datan kan påverka din, men även även hela hushållets, personliga integritet i framtiden?

(U)
Nej det har jag väl inte. Eller i för sig, man förstår ju såhär att den kan ju ha koll på mina matvanor genom att va kopplat till mitt kylskåp till exempel. Men ja i the long run, kan ju mina beteenden utnyttjas åt kommersiella intressen som jag kanske inte vill. Det kan utnyttja på rädsla till exempel om det är någon som köper väldigt mycket råttgift och det kommer fram och sen så blir det mycket reklam om att det är väldigt mycket råttor och såhär för att man ska bli rädd för det till exempel. Så att absolut. Just nu så tror jag inte det är på den nivån, men jag tror lätt det kan vara i framtiden. All rörelse och allt som händer i ett hushåll, kan liksom bli utnyttjat av andra intressen för den information som spricker ut.

(I)
Okej, och vet du vem som äger rätten till den data som samlas in av företagen?

(U)

Nej.

(I)
Är det något du har försökt ta reda på?

(U)
Nej.

(I)
Finns det någon orsak till att du valt, eller försökt, att inte ta reda på det?

(U)
Det är en kombination av… Alltså lita att jag tycker att vissa grejer är rimligt, information som samlas in. Som jag är okej med. Alltså jag är okej med, till exempel om jag söker på internet eller vad man än gör och det kommer upp reklam om vad jag har sökt och så vidare. Och att jag har lite förtroende för myndigheter och för företagen, jag tänker att de kan. Att de blir granskade och så vidare. Men annars så är det väl en [...] och brist på kunskap liksom.

(I)
Yes. Och sen, med rätten till data och att det är någon som har den eller vem det är som äger rätten till den. Vet du vem som har, eller vilka som har, tillgång till datan när den är insamlad?

(U)
Alltså i Alexas fall kan jag tänka mig att Amazon har tillgång till den. Sen typ… nej. Alltså jag förstår att företaget som producerar enheten i sig har delvis tillgång till den datan den samlar in. Men sen när det kommer till andrahands- eller tredjehand-saktörer så har jag ingen aning om hur de använder datan sen. Och vilka sen har rättigheter till den. Till exempel. Så nej jag har ingen större koll på det liksom.

(I)
Mm. Anser du då, till exempel att enheterna har tillräckligt med begränsningar för olika behörigheter? Om man tänker i hushållet till exempel? [...]

(U)
Nej alltså just nu är det inte så [...]. Men jag tror att man kan göra en del grundinställningar. Den som är admin till exempel, att den får begränsa funktionaliteten. Men sen kan alla använda det som är användbart. Så det är väl både och där. Och sen är det ju inte helt klart heller hur den här Alexa får kontakt med alla de andra enheterna, hur den hittar dem och sådär. Utan det är bara "what, oj den hittat någon strömbrytare" liksom. Så nja, lite både och tror jag. Man kan ju göra

bakomliggande inställningar och såhär men man kan ju inte förhindra dem från att använda någonting. Det är ju inte såhär, alltså om vi säger att du kan sätta på spisen med min smarta enhet så kan du aldrig hindra något barn från att gå och göra det. Det går ju inte att säga "nej tyvärr du måste vara över 18 för att kunna göra det här" liksom. Just nu i alla fall.

(I)
Yes. litar du sen då på att de enheter du använder funkar som de ska?

(U)
Nej det gör jag inte. Alltså jag tycker inte att teknologin är så pass bra heller [...]. Jag tycker det är häftigt och kul när det funkar, men jag tänker att det funkar lite knaggligt liksom. Jag hade ju inte satt mitt liv i deras händer över huvud taget haha, så kan man säga.

(I)
Haha okej. Men anser du då att det finns några risker med till exempel din data som finns där kan bli manipulerad?

(U)
Ja det skulle jag säga, med tanke på, alltså jag tror så här det är väldigt avancerad tekonologi som hanterar väldigt mycket data. Du måste vara ganska duktig själv på tech och grejer för att kunna förstå och begränsa de här enheterna för att göra som du vill och kan förstå riskerna med det. Förstår du inte detta, så tror jag det kan vara väldigt väldigt enkelt att utnyttja. Och som andra kan få tillgång till den datan och handha den på olika sätt. Så jag ser ju definitiva risker med det så att säga.

(I)
Yes. ser du några andra risker för hushållet vid användning av smarta enheter, just personlig integritetsmässigt?

(U)
Ja alltså [...] allting är uppkopplad till internet, det är det det handlar om. Alltså det finns ju tydliga säkerhetsrisker i form av folk som är hackare till exempel som kommer in och kan helt plötsligt styra vårt hus. Alltså jag vet inte hur mycket du kan manipulera de här enheterna, men de borde säkert kunna göra ett strömavbrott eller vad som helst. Eller sätta på massa saker samtidigt. Alltså den typen av säkerhet, för det första tror jag inte man sätter på den själv. Så det är svårt att veta vad som är bra och vad som är dåligt. Och för det andra så är ju internet där, internet överlag är väldigt liksom sårbart för säkerhet för det finns väldigt duktiga hackare och så som kan komma in. När de kommer till exempel till säkerhet till din dörr så kan du ju fatta att "okej, har du världens sjukaste lås här så kan de inte komma in" för de har liksom inte, alltså det

är väldigt väletablerat och forskat på hur kan en tjuv komma in i ditt hus till exempel. Men i de här fallen så finns det inte det. [...] Då tror jag framför allt att tredjepartsaktörer som är hackare liksom, som kan gå in och styra ens hus, samla in information om en själv. Det kan vara kriminella nätverk eller vad som helst som kan förstöra.

(I)
Yes. Vilka skulle du då säga är de största riskerna kring detta?

(U)
Alltså största riskerna det skulle jag definitivt säga, jättestora eller olika typer av företag för ett liksom icke-moraliskt sätt använder och tar information. Så de sprider för att utnyttja dess användare för att tjäna pengar liksom, på olika sätt. Som användarna själva inte förstår hur der används, på vilka sätt der tas in och så vidare[...]. Och det andra är definitivt att med hacking attacker och så vidare [...]. För det vet jag såhär att det finns ju exempel om du går in i smarta hem och utför till exempel processorn från en smart brödrost. För att använda den, den processorkraften till en hacking attack någon annanstans till exempel. Så det finns att andra människor kan få tillgång och styra ens hem och sen så man själv inte kan styra det. Eller om, när det är manuellt så måste du vara fysiskt närvarande liksom. Och att de kan ta in information om dig själv och dina grannar för att, ja använda den på olika typer av sätt, det kan va utpressning eller vad som helst liksom. Det är väl de två största riskerna. Och kanske till och med liksom såhär främmande regeringar som samlar in informationen, så jag menar det finns väl inga begränsningar liksom.

(I)
Mm nej men precis. Påverkar riskerna valet av vilka enheter du väljer att använda dig av?

(U)
Nej inte i nuläget. [...] Man kommer väl reagera när man börjar ser problemen. Men just nu är det väl mest en häftig apparat som hjälper en. “Lampas ska släckas klockan åtta” och sådär och tändas lite då och då. Så att nej, just nu gör det inte det. Men jag kan tänka mig att det kommer göra det i framtiden faktiskt.

(I)
Mm, och är det då liksom, på grund av att ni anser egentligen då att vinsten är större än riskerna då eller?

(U)
Att jag fortsätter använda dem nu är nämligen att, det är ju lätt att man tänker att det blir konspirationsteoretiskt när man tänker att “åh fan vem lyssnar på oss, vem gör inte det?”. Så man

väljer liksom att va lite naiv och lita på myndigheter och lita på företag och regelverk och lagar och så vidare, att det fungerar. Tills det inte gör det och man kan se de obvious riskerna [...]. Att spelar den in all information som man pratar om så kan det ju bli farligt, men det tror vi liksom inte att den gör, förutom när man ber den att lyssna på vad man säger och sådär. Och då använder vi ju inte på ett sätt heller som skulle säga, är liksom kritiska eller vad, utan är bara till "sätta på lampan" eller "inte sätta på lampan", "sätt på min spotify" kanske och så vidare. Men desto mer den liksom tar över vardagsfunktioner och sånt, och är man säg exempel på verkligen risker med detta, desto mer kommer den bli medveten.

(I)
Mm yes, och den data då som samlas in av de här enheterna, anser du att den alltid är tillgänglig för dig som användare när du vill ha den eller behöver den? Alltså använda olika funktioner, eller använda datan till någonting?

(U)
Nej. alltså ens egna historik om vad man hanterar, jag vet att vissa typ produktioner och så vidare samlar in och du sen kan titta på vad ungefär de tycker och tänker. Men det är väldigt svårt att hitta det. Jag tycker inte det är transparant.

(I)
[...] Finns det någon typ av information eller data som skulle resultera i att du slutar använda vissa enheter, eller någon specifik enhet?

(U)
Ja alltså, du menar om man skulle på reda på att den har en viss typ information om mig?

(I)
Jo precis, alltså om det är någon specifik data om dig som den samlar in som du känner att, nej okej nu vill jag inte använda den längre.

(U)
Ja alltså så fort den blir liksom personlig, emotionell, saker och ting som man kanske inte vill att man mår sämre eller man fruktar någonting, man vill hantera det. Eller någon psykisk ohälsa. Eller bara egentligen personliga grejer, åsiktsregistrering, vad som helst. Då skulle jag reagera väldigt väldigt starkt. Den typen av grejer skulle jag inte ta med. Utan i så fall ska det vara väldigt tydligt, för att jag har inget emot att reklam är riktat. Om det är så att jag har ett cykelintresse och den ger mig alternativ till bra cyklar till exempel. [...] Men absolut, så fort det liksom blir personlig och det inte handlar om marknaden liksom, då skulle jag definitivt börja

agera mot det liksom. För att man vill ju inte att den ska se allting man googlar eller alla intressen man har och allt sånt där.

(I)
Och om man kollar då, de smarta enheterna kan man dela upp i fyra områden. Och då har vi energi, hälsa, säkerhet och underhållning[...][6]. Vilken av de här områdena skulle du säga är, eller klassificera som mest känslig i förhållande till din personliga integritet?

(U)
Alltså då tror jag ändå att, underhåll känns ändå relativt okej tror jag. Hälsa definitivt, även säkerhet för den kan liksom registrera mönster på något sätt och det kan vara information som är liksom betald för en själv. Att man vill känna sig väldigt väldigt trygg. Och sen var det energi också pratade vi om va?

(I)
Ja precis.

(U)
Ja. Den är också, alltså jag tänker allting som styr dina vardagsfunktioner i form av att, som du måste förlita dig på att, det verkligen fungerar. Där finns det liksom risker. Men jag tror framför allt säkerhet och hälsa. Den information borde inte komma till någon som inte ska behöva det liksom. Och även [...], alltså underhållning kan ju på något sätt läsa av att denna människa är väldigt deppig, den lyssnar deppiga låtar. Alltså vad som helst. Man kan få ut väldigt mycket av en människa, både på vilken typ av underhållning man håller på med och sådär. Så det är ju alltid det här metatänket kring vad säger detta om personen, och det kan man nog få ut lite av allihopa. Men framför allt när det kommer till såhär betalda trygghetsfunktioner, så säger jag mest säkerhet på dem [...].

(I)
Mm, är det både om du tänker då kortsiktigt och långsiktigt. Är det samma då eller?

(U)
Aa jag tror långsiktigt, långsiktigt framför allt så är det med liksom hälsa och säkerhet. Och även kanske till och med energi, alltså för det kommer nog bli väldigt mycket smartare och ersätta de vitala funktionerna. Underhållning, alltså underhållning med människor har men det är liksom inte Pavlovs behovstrappa. Såhär, det är inte att du dör inte av om du inte fixar underhållning manuellt på samma sätt. Men desto mer liksom det automatiseras och tar över alla de här

[6] Begrepp förklaras för intervjuperson

säkerhetsfunktionerna, får du mindre kontroll än vad du borde lägga på trygghetsgrejerna liksom. Och det har det inte gjort än hundraprocentigt, men jag tror det kommer komma i framtiden. Att liksom att du vet liksom inte om hur du säkrar ditt hus utan det är någonting i molnet eller vad som helst, till stor del liksom.

(I)
Ja men då får vi tacka så mycket för att du tog dig tid.

7.2.8 - Företagsrepresentant (IPFR)

Datum: 2018-04-20, 11:46-12:39
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Men jag tänkte, vi kan ju börja med att jag sätter igång den här. Vi kan börja med egentligen gå igen exakt vad vi gör då, för att göra klart för dig. Som sagt vi kommer ju då från Lunds universitet, vi läser sista året systemvetenskap, och nu så ska vi göra en kandidatuppsats där vi har fokuserat på smarta hem och dess enheter och hur allting i i smarta hem påverkar den personliga integriteten vid datainsamling och datahantering och behandling och ja det är väl lite det som är syftet att vi vill se vad för typ av data som samlas in och vad man gör med det och sen hur det hur det används. Och vi har ju redan gått igenom det nu lite innan då men eh vi egentligen då vad för smarta enheter som ni jobbar med och vad ni säljer, vad det är för något.

(U)
Ja alltså vi vi har två olika två olika system eller två plattformar då, en plattform som heter Connexoon och det är en ren appstyrning kan man säga. Det finns inget webb interface, ren appstyrning då. Och en appstyrning för man kan säga solskydd är vår produkt då. Det är markiser och [...], gardiner, persienner, etcetera. Man kan även styra Philips ljusbelysning. Allting trådlöst då, det är det ena systemet [...]. Och sen vårt riktiga smarta hem systemet heter Tahoma och det

är ju också då en hub, men förutom vår egna produkt, som jag precis rabblade, instegsprodukten, så kan man då styra även andra partners produkter. Man kan röststyra det via partnerskapena, med Amazon Alexa, IFTT, och via IFTT även Google Home, vi kommer bli kompatibla med Apple Home Kit, eftersom att om allting blir som det ska med apple, är med och spelar på det, vi är kompatibla med till exempel, SONOS musik, när det gäller musik, vilket innebär att när man kommer hem, öppnar dörren så kan ens favorit spellista dra igång, eller att man länkar musik direkt till en automatisk körning vid en speciell tidpunkt, så det verkar som att du är hemma till exempel. Kan styra temperatur i huset via två olika system. Ett från honeywell och ett från Danfors. Så, det är omöjligt idag och ha liksom alla grejer för att styra ett hem, man måste liksom connecta med andra externa partners då, vilket det är inte helt enkelt, men många av dem här systemen, typ IFTTT, gör att det blir ganska mycket enklare, så det är ju som via tredjeparts appar eller via tredje parts system, som blir mer och mer kompatibel kan man säga, och det är det folk vill ha idag, och inte att förglömma naturligtvis, kameror i hemmet, vilket verkligen inspelar på den personliga integriteten, kan man säga. Det är ju mycket intressant grejer, med just kameraövervakning och där får vi mycket frågor runt kring det också från från privatpersoner, som undra hur det fungerar. När man då köper den där själva boxen, själva hårdvaran då, så pluggar man in den då i sin router som man har hemma, som de flesta har idag, och sen skapar man som många andra företag användarkonton på vår hemsida, inget konstigt egentligen, i det här användarkontot då så man skapar så anger man en emailadress och naturligtvis föreslå ett lösenord och där har vi vissa krav på på hur lösenordet ska vara, det står framgår i vid registreringen då naturligtvis, och sen så knappar man in sitt namn naturligtvis och adress och så där. Men email och password är det som är nödvändigt, inga personnummer, sådana saker. När man sen har gjort det, så får man ett mail från systemet, då man får godkänna, så det är liksom en standardprocedur, för hur det ska fungera [...].
Den där boxen, länkas upp mot flera server i som står i Frankrike. [...] Den där kommunikationen mellan boxers och servers är det som gör att systemet fungerar, så tappar man internetuppkopplingen så fungerar inte systemet längre så att säga, man måste ligga uppkopplad mot, mot internet helt enkelt. När man sen programmerar ganska enkelt då, vilket du gör själv [...] i systemet att det ska vara väldigt enkelt, så simpelt. Det finns liksom egentligen ingen direkt manual utan mer liksom självlärande och dem eventuella programmeringar man gör till exempel är, tänder lampa kl 6 på kvällen [...] alla dem programmeringar, om du tappar internet uppkopplingen mot servern, så ligger dem sparade i boxen, lokalt också, då körs dem körningar ändå fast du tappar uppkopplingen. Det du inte kan göra är att du kan inte överstyra körningar via telefonen för dem måste, de måste vara uppkopplade, men automatiska styrningar funkar fortfarande, som ligger på hubbarna. Systemet har vad kan man säga, en krypteringsnyckel då och i boxen så finns det, som det ser ut just nu iallafall, ett “tre styrprotokoll”, iallafall. Tre som fyr styrprotokoll kan man säga. Två envägs som sänder iväg en signal [...] Ett tvåvägs protokoll som sänder iväg någonting och produkten sänder tillbaka en signal, vilket gör att man får feedback i systemet, så man ser till exempel fönster stängt eller markis är uppe, garageport är låst

osv stängd. Belysning tänd [...]. Kaffekokaren är avstängd, strykjärnet är avstängd sådana saker, vilket man har stor nytta av beroende vilka typer av produkter och priser. I den där tvåvägs systemet, dels är det ett protokoll [...] kan man säga. 16 miljoner olika kodar, sedan 32 bitars krypteringsnyckel, som systemet får. Och detta systemet, eller den nyckeln, är uppenbarligen taskig att hacka, det går inte än så länge. Nu är det så att varje år så hyr vi ett sånt där hackningsbolag som heter [...], som försöker hacka systemet. Ta sig in, och än så länge har dem inte lyckats med det. De har gjort det 3 år i rad. Så vi har ett sånt där certifikat vi skyltar med på hemsidan och så där. Det är ganska viktigt. Många system som idag finns på marknaden är inget speciellt säkra.

Så att det är nyckel då. Det jag kan säga med det också är att det är ju mycket skrivs ju mycket om detta, säkerhet och kameror och sådana saker. Jag kan ju köpa en kamera för bara några hundralappar, på typ Kjell och company eller på vilken internetsajt som , hur pass säkra är dem liksom? Folk tänker ju inte på det alltså . Jag menar man har ju ingen aning, och i och för sig, med tanke på Facebook och andra sådana här plattformar, verkar folk struntar i det exempel haha. Folk vill gärna visa upp sig eller något sånt, eller vet inte, men vi får faktiskt en hel del frågor av folk som kommer in här [...]. Men de som verkligen är intresserade och kommer hit här, de har mycket frågor kring säkerheten. Speciellt när det gäller kameror [...].

(I)
Jag tänker lite är frågorna ofta riktade mot externa hackare, för jag tänker också på hur företagen behandlar dessa uppgifter, om man är rädd för detta.

[...] Det kan det nog vara både och, men framförallt så är det kanske är frågor som till exempel, om jag köper ert system, den här kameran, kan ni gå in och kolla på den? Ja alltså den typen av fråga, det är det ju lite intressant. Alltså jag har av naturliga skäl inte andra system hemma då, men till exempel mina föräldrar har system från Verisure. En av mina grannar har också, med kameraövervakning då och när om man till exempel har en brandvarnare i köket, och du står och steker någonting och så blir det väldigt mycket av någon anledning mycket rök, då går ju brandvarnaren naturligtvis. Och då får ju centralen som det är kopplat till får ju en länkar om det, då går ju dem in och kollar i kameran och då har vi haft ett antal här, som kommer in här och som inte uppskattar det då, för alltså även om man skulle kunna gå in och kolla på kameran så får man inte lova att göra det. I det fallet får du ju göra det och då har du ju signat off för det i vad ska man säga i de legala dokumenten som du skrivit i när du har köpt systemet. Jag tror det är många som till en början inte tänker på det, men när du har väl installerat och efter ett tag sitter det där en nisse där nere och kollar nu på mig liksom när jag sitter där i kalsonger liksom, alltså du vet [...].

(I)

Men jag tänker också då lite såhär har man någon slags behörighet för dem som får kolla i dessa kameror?

(U)
ingen ingen aning, jag vet inte alls hur det funkar, det har jag ingen aning om hur det funkar, bara fått massa frågor om det dära, och själv börjat tänka. Ja det kanske inte är så himla kul. Vi har också förutom dem här smarta hem system så har vi även ett , vad ska man säga, ett larm med appstyrning kan man säg. Där istället för ett enkelt hemlarm så att säga och istället för att det är uppkopplat till central då så har man själv kontrollen över det. Plus att man kan ha en community istället, grannar och föräldrar och kompisar och så där som är inkopplade på ditt eller ditt eller mitt larm då, så går larmet och jag är i Stockholm så så får även min granne larmet då kan han liksom hjälpa till och så där. Men då har vi ju själv koll på det, då kan man själv ge access och gå in och kolla på kameran, du vet ju liksom det är begränsat och du har själv koll. Dessutom [...] på de kamerorna så är här finns där en en sån här liten lucka som när så fort man kommer in inom dörren eller via gps när hundra meter från nu så typ när du kommer hem så att säga, så stängs luckan för linsen för kameran. Man behöver inte ha det så, men det är förinställningar. Så när du kommer hem så filmar den inte, så kan du aktivt starta den om du vill att den ska filma, det kallas för privacy chatter på engelska , vet faktiskt inte vad det heter på svenska. vad vi kallar det på svenska. Men asså just för den här alltså den privata delen, när du är hemma så vill inte du bli filmad, nu kan vi ju ändå inte gå in och kolla på den men, många har en känsla när du har en kamera, så ser du kameran, tänker du “mhm vem kollar på mig nu?”.

(I)
Men jag tänkte också på det här krypteringsstandard som ni säger att ni använder er av, är det då främst eller är det enbart då liksom lösenord och hela den biten då eller är det även videoströmmar eller annan data som samlas in för att automatisera det smarta hemmet?

(U)
Alltså den nyckelen, krypteringen ligger i själva systemet.

(I)
I hela systemet?

(U)
Ja, så att det är inte bara mellan fjärrkontroll och en motor till exempel, utan det är hela systemet som sådant. [...]

(I)

Så all data som samlas in liksom, behandlas likadant egentligen?
(U)
Ja och där är det så att jag då sitter på vad ska jag säga, försäljningsbolaget i norra europa. Och är ni intresserade att få reda på mer hur tekniskt perspektiv, mer på djupet, kan inte jag det. Men då kan jag säkert länka vidare till kollegor i frankrike, om ni har behov av det. Jag vet inte hur pass djupt ni behöver gå in i detta och jag vet inte hur pass mycket de kan lämna ifrån sig osv men det gör jag gärna om ni behöver det och jag kan ju berätta lite vad jag vet vi använder data till, men i detalj hur det fungerar och hela biten, det kan inte, för jag helt enkelt inte vet det.

(I)
Absolut det är ju förståeligt

(U)
Men om vi ska gå in på just det när det gäller datan. Vad ska man säga, det vi använder datan till, som vi samlar in, det vill säga det som samlas in och loggas det är ju inte jättesexiga grejer om jag säger så, iallafall inte ur ett, om man tänker sig ur ett försäljningsperspektiv. Utan det är mer ur ett användarperspektiv, kan man väl säga, om man då till skillnad från till exempel Google, Facebook och sånna saker och dessutom så får vi absolut inte sälja det vidare för tredje part. det står också i dokumentation som som man signar för när man köper systemet, men det som det som samlas in och loggas är ju hur och när man till exempel kör ner rullgardinen när man tänder en lampa och sådana grejer och hur man använder det och hur ofta man använder det. Sen utifrån det, den data, tar vi sen beslut om vi ska utveckla fler produkter och andra produkter och gör en twist för att den vi har vi har en feature på en produkt till exempel, att den här lampan ska dimmas den har mottagare [...]. Och så visar det sig att alla som använder den produkten, använder den bara som on off till exempel eller, då kanske vi inte behöver utveckla fler dimmers. Som det ser ut som de, alltså typ sånna grejer, vi använder helt enkelt för att förstå våra användare har för behov helt enkelt. Men i detalj så som man kan säga även användare som sådan, de använder systemet, har ju tillgång till till en logg då. Så startar jag min app här [...], så har man ju en logg här, och det är så att säga denna loggen sparas på servern då.

(I)
Så då är det rätt så transparant för kunden, då ser man själv också vad som loggas, Eller?

(U)
Exakt! Och det kan man ju ha nytta av till exempel om man har till exempel satt som, jag har till exempel ett garage hemma med en garageport och så har jag då en garageportsöppnare, som är det här tvåvägssystemet, så man får feedback, så nu ser man att den är att den är låst. Att den är stängd, så kan jag då öppna härifrån då, så nu öppnar jag garaget där hemma, och då sänder den tillbaka. Så nu kör den upp då så, så om en stund så kommer den att stanna [...]. Så och då ser

man, får man feedback direkt i koden. Ser man att den är öppen, den biten där. Hade det varit ett envägs så hade man inte fått det. Då vet man att den är öppen, men du vet inte hur mycket öppen och om den är öppen. Nu vet jag att den är öppen då. Den informationen kan man sen då hitta. Garageport 45 % och den är den är gjord med en iphone då. Så den feedbacken kommer upp direkt då. Så det är helt transparant på det viset.

(I)
Men jag tänker på till exempel med det här du sa att ni inte säljer vidare till en tredje part. Men om ni då använder liksom, vad heter det, om ni då, om ni ansluter andra produkter med ert system, då får dem ju den datan där, det skapas kommunikation mellan dem väl?

[...], det vet jag faktiskt inte hur det funkar. Om dem kan se den information också, jag vet inte, det tror jag faktiskt inte. Det är ju vårt system. Så att det kan jag inte tänka mig att de kan se, möjligtvis, dem har eget system då, som man till exempel Philips Hue, som är det här belysning, vad heter det smart belysning från Philips, har jag ganska många sånna lampor där hemma, så de ligger här. Alla dessa här då och då är det ju som så, när vi , när vi länkar ihopa oss med Philips, så länkar vi inte ihop oss med varenda lampa här. Utan då länkas vi ihop med deras brygga, som de kallas de, deras hub kan man säga, så vår hub och deras hub via API uppe i molnet, det är molnet som pratar med varandra.

(I)
Okej

(U)
Vår data har vi, deras data har dem. Så dem får ju samma data som vi. Men det är inte vår data utan det är dem själva som samlar in liksom. Men just det här, det höjs en fråga som vi har, vi från försäljningssidan har tagit upp själva, till exempel alltså när det gäller säkerheten, speciellt då med dem här systemen som röststyrningssystem, som Alexa och Google och så ju mer man liksom öppnar upp sig ju mer sårbar blir man då [...]. Det ska bli intressant nu när de ska försöka ge sig in och hacka systemet. om det har några förändringar i systemet, jag tror inte det, men jag hoppas inte det, men det vet man ju inte liksom, det är också en fråga som vi får. Ju mer vi expanderar ju sårbara blir systemet, mer komplext blir det på det viset. Men fransmännen brukar ha bra koll på läget, de är extremt noggranna ehh att saker och ting fungerar och testar, men visst, det är ju större ju större mer komplexa vi blir, ju svårare är det att hantera minsta lilla detalj i det, så enkelt är det. Och sen är det ju dessutom så att när det gäller, kanske inte säkerhet så, men när det gäller datasäkerhet eller personliga datasäkerhet så är det ju det här nya som träder kraft nu i Maj, den här GDPR, och det vet vi än så länge inte exakt, hur vi ska hantera, ännu faktiskt [...]. Åker man dit då och har inte koll på läget, så ryker man [...]. Så det är mycket snack om det i företag just nu, samtidigt så är det lite speciellt just med dem här bitarna för att

här måste vi ha kontinuerlig kontakt med våra användare här eller uppdateringar och så, informera dem om uppdateringar. Men alla dem här data, som vi har på varje användare, dem måste vi ju ha annars kan de inte använda systemet, så att det är ju lite speciellt på det viset.

(I)
Men som jag förstår det, då är det själva överföringen sker via molnet, och sen så lagras det via servrar i Frankrike. Är det någonting som stannar i molnet? Finns någon backup-lösning uppe i molnet också eller?

(U)
Den eeeh, tekniska infrastrukturen har jag ingen aning om alltså. Det måste jag säga, tyvärr, behöver ni veta sådana saker så kan jag försöka ta reda på det eller bästa hade ju varit att länka ihopa er med fransman.
(I)
Det vore ju jätteintressant också om det går, absolut.

(U)
Jag kan slå en pling i eftermiddag. Hur och vem det är som skulle kunna vara så i såfall om de är pigga på det.
(I)
Ja såklart. Som sagt vi förstår självklart att man inte kan gå ner i superdetaljer med krypteringsstandarder och liknande.

(U)
Det hade kanske kunnat vara intressant för er ändå att få kontakten jag vet inte, jag vet tyvärr inte de detaljerna.

(I)
Men absolut, det är ingen fara. Jag tänker lite så här, överlag nu med det här med smarta hem, alltså vart ligger typ fokus med om man tänker så här, man vill ju utveckla ny produkter, tänker man mycket på att det ska liksom möta kunders behov eller att det ska vara så säkert som möjligt. Liksom vilket fokus brukar man gå in på. Man vill ju göra allting så enkelt som möjligt, då blir man också lite, tänker man på säkerhet?

(U)
Ja, ja det beror på lite vilken produkt det är kan jag ju tycka. Till exempel, de här kamerorna, som för vår del är ganska nya då, då är det ju just det här med säkerheten.

(I)

Säljer på?

(U)
Jag tycker är viktigt liksom, och ja det är ju huvudargumentet, precis [...]. När det gäller typ lås, alltså när du har lås och den typen av lösning, så är det ju extremt viktigt. Eller som den här garageporten till exempel. Vissa hus har garageport som en dörr in till huset också, så funkar inte det så är det ju katastrof alltså. Så att det beror sig på vilken produkt det är kan jag tycka.

(I)
Såklart.

(U)
Och när det gäller dem bitarna så, vi som bolag, kvalité är ju vår viktigaste grej. Så vi lägger ner enorma, enorma resurser på testa och sådana saker. Inte vi här då utan på frabriken. Så att det läggs ner mycket pengar och tid på att se till så att saker är säkra, speciellt de här säkerhetsprodukterna. Typ garageportar, grind, som är väldigt stort nere i Europa och inte så stort I sverige än så länge. Blir ju mer och mer populärt att man liksom stänger av sin trädgård för att folk inte ska komma in. Vi är mer öppna. Och sen larmgrejorna liksom det är enormt viktigt. Så att, annars är man ju rökt alltså. Problemet är ju att har man inte koll på det där och man kommer ut på marknaden, nåt sånt här brett liksom och det skulle krascha, så går det ju på någon dag sen är man helt borta liksom. I och med Facebook och alla sociala, vad heter det, flöden som finns, så är det ju extremt sårbart. Det är nyckeln till succé att man har liksom upp-backat.

(I)
Jo precis, så är det ju. Sen tänkte jag lite såhär, har ni då behörighet till att, eller har ni olika behörigheter till att gå in i...

(U)
Administrationsverktyg?

(I)
Ja precis.

(U)
Yes det har vi, så vi kan göra en viss del av support här mot våra användare. Och sen så när vi inte kan göra basic grejer så har vi, kallar det ticket-system, vi anmäler ner till Frankrike, så sitter där som liksom en second line. Liksom som de flesta bolag har och där är det som så att de bara får göra grejer under förutsättning att vi har en konsument som frågar efter, eller har ett problem.

Vi får ju inte gå in och ratta med konton och sånt om inte konsumenten har godtagit det. Om det inte fungerar så har de ju ett problem, så får vi ju lösa det så att säga. Så vi har ju två två killar här uppe plus mig själv som kan göra en viss del då på ganska låg nivå, och sen så de flesta grejer skickar vi ner till till Frankrike. Alltså jag tror de flesta har den här setupen som vi har. Alla som har en liknande verksamhet, har väl också en firstline support och sen en seconline, när det krisar liksom.

(I)
Mm precis. Jag tänker med den data då som du sa loggas som ni har, är det någon data som används för att hjälpa er också, till exempel förutspå trender?

(U)
Ja det är det ju, så vi får ju det en gång i kvartalet eller två gånger om året. Då får vi liksom feedback tillbaka, som säger ja i Sverige så ser det ut så här. Så här många markiser är uppkopplade [...] och så kan man då ju jämföra länder mot länder och delar av Europa mot andra delar av Europa och så vidare. Och så kan man ju se trender och så.

(I)
Är det någonting som ni känner har hjälpt er mycket då?

(U)
Än så länge inte, för tycker vi har för låg volym än så länge kan jag tycka. Men man ser ju ändå åt vilket håll det verkar liksom. Det vi ser här uppe är ju att belysningen till exempel är en nyckel. Alla användare har ju uppkopplad belysning i vår system. Det står ju att många har markiser för det är det som är det stora här uppe, medan i Frankrike så är det mer säkerhetsprodukter kanske. Som jag nämnde grindöppnaren, men kanske inte så mycket belysning [...]. Men på övriga produkter så kräver det större volymer och än så länge är vi inte riktigt där. Med antal användare och så vidare så. Man får, i Frankrike som är vår hemma marknaden, där är dem ju enormt stora och där kan man ju se grejer. Oftast kan vi inte riktigt dra nytta av det för att de lever helt annorlunda än vad vi gör. Det är en helt annorlunda kultur, så vi kan liksom inte riktigt dra något från det. Fast det är ju det som är en av dem bra grejerna med det. Och sen är det ju så också att all den där statistiken, ja visst den samlas in, men i det sammanhanget så är den ju väldigt generell, man går ju aldrig in på individnivå. Tror vi är annorlunda. Om man samlar in data för att sen kunna sälja grejer till alltså. Du använder en produkt på ett visst sätt, du använder en produkt på ett visst sätt och jag använder på ett visst sätt. Så beroende på mitt användande, så kan jag skicka ett erbjudande till dig. “Jag ser att du använder musen ofta” om man nu kunde se det, “Men den måste vara sliten, så här får du ett erbjudande om en ny mus”, alltså den typen, det är ju inget vi sysslar med något överhuvudtaget.

(I)
Mm okej.

(U)
I alla fall inte än så länge och jag har inte hört talas om att det ska bli så heller, men det finns ju många som gör det. Till exempel Google och så.

(I)
Mm precis.

(U)
Så att det är ju inte det som är vårt syfte.

(I)
Nej men precis, det är ju rätt så vanligt att det faktiskt händer, speciellt med större företag tror jag.

(U)
Ja, det viktigaste för oss är att alltså detta är ju ett fokus som vi har nu inom företaget det är ju att, vi vill så att säga, koppla upp så många användare som möjligt ehh för att just få in all den här data, for att kunna se hur våra produkter används. Så att vi kan göra det bättre .

(I)
Ja precis.

(U)
Det är det som är huvudsyftet med det och jag tror att innan så hade vi ingen aning liksom. Eller ja det hade vi, vi gjorde ju surveys och sånt, det gör vi fortfarande.

(I)
Men det är enklare nu med all data?

(U)
Ja, ja det är ju faktiskt det.

(I)
Men då vet du inte hur länge datan lagras i typ servrarna, eller ja det vet du inte.

(U)
Det har jag ingen aning om, vill ni att jag ska ta reda på det?

(I)
Ehm om det är någonting som kan tänkas påverkas av GDPR som träder kraft? - T,

(U)
Ingen aning [...], det är möjligt att det gör det. Som jag har förstått det så är GDPR mer om till exempel jag skickar, jag ringer ett bolag, ett försäkringsbolag till exempel som jag inte har, jag är inte ens kund där. Och så frågar jag dem några grejer, så tar de mina uppgifter och kanske skickar en offert till mig eller så, och så signar jag inget. Då är den restriktion på hur länge de får ha den datan. Jag tror det var tolv månader sist jag hörde det. [...]men det är möjligt att det är så här också. Jag har ingen aning, men intressant fråga.

7.2.9 - Svenska Säkerhetsmyndigheten (IPSS)

Svensk Säkerhetsmyndighet - Intervjuperson X (IPSS)

Datum: 2018-05-02, 15:12-15:48
U: Uppgiftslämnare
I: Intervjuare

INLEDNING

- Berättar om anonymitetsskydd.
- Frågar om vi får spela in.
- Presenterar oss kort.
- Förklarar syftet med intervjun.

INTERVJUSTART

(I)
Skulle du bara lite snabbt då kunna berätta om din yrkesroll för oss?

(U)
Mm absolut. Ja jag jobbar som, den tråkiga versionen är handläggare, det roliga är internetinhämtare. Så jag bevisar egentligen mycket material på nätet, sociala medier och olika forum. Spårar och kartlägger och där har vi nått vad information och vad är rätt och vad är inte rätt och så där. Jag jobbar med det sen 2007 och har varit här på samma ställe.

(I)
Yes, hur skulle du definiera personlig integritet?

(U)
Det är väl information, det är svårt fråga. Eller ja den är lite klurig, men ja. När det gäller data och sånt, vad man lämnar ut och vilka andra som får access till den information som jag lämnar ut om mig, hur kan man bygga ihop allting så att det kopplas till mig. Vad lämnar jag ut och vad lämnar jag inte ut? Ja, vi börjar där.

(I)
Men vad ser ni verkar vara den största orsaken till identitetsstölder? Finns det någon mönster bakom det?

(U)

Ja eller mönster, jag tror att folk är lite rädd, eller de tänker det händer inte mig. Sen är man väldigt slarvig med lösenord. Man har enkla lösenord, man tänker inte hur man behandlat sina uppgifter eller hur man loggar in. Och det säkerhetstänket med att ju mer information som man använder, mer appar man använder, blir mycket mer information som man ger ifrån sig. Och jag tror det där att folk är så slarviga med lösenord att man byter inte lösenord och man är inte rädd om det. För man tänker hela tiden det händer inte mig. Det har jag själv fått höra, du måste byta lösenord och om du ska ha ett särskilt security-konto och gå vidare sen, för att återställa med lösenord. Men då tycker man det är så jobbigt att byta lösenord på två konton och då har man samma. Man förstår inte den risken och hur lätt det är att ta det av information som folk bara släpper ifrån sig.

(I)
Mm. Vilka enheter just i det smarta hemmet, tänker du kan vara mest utsatt för sådana här externa attacker?

(U)
Det spelar egentligen ingen roll, för så fort du är uppkopplad mot nätet så finns det ju en risk att bli hackad, komma åt lösenord. Men oftast absolut. Som bredband, ditt bredband, du byter inte lösenord när du skaffar ett nytt bredband, det är ganska lätt att komma åt. Och då kommer du åt alla enheter som är inkopplade på det bredbandet i det trådlösa nätverket. [...] Garageportar, till och med bilar har internetuppkoppling, så allting som är kopplat mot nätet, sen visst, hårdare krypteringar och svårare att knäcka vissa krypteringar, absolut. Men det som är uppkopplat är ju uppkopplat. Bara det att, hackare de ligger ju alltid, eller alltid det ska jag ju inte säga, men de ligger steget före. Det är ju deras jobb, för att utmana krypteringar, att hitta säkerhetshål för att kunna komma in. Det är alltid en kamp där. Så nej. Om det hade varit kylskåpet eller kaffebryggaren som skulle bli hackat, nej jag kan inte se något som är värre än det andra.

(I)
Aa okej. Finns det någon data som samlas in som kan vara mer känslig då? Som är utsatt kanske eller så?

(U)
Ja men som hemlarm, till exempel. Ja för hackar du in på det så kan du ju slå av larmet sen när du ser att dem har larmat på och folk är inte hemma, till exempel. Då får du inbrott i huset. Nä men ja, men sen sitter ju folk oftast med information på sina datorer, sina paddor. Det är där man vill komma åt det. Misstänker jag iallafall. För det är där du hittar lösenorden, bankID [...].

(I)

Mm och om man vänder det till säkerheten för den personliga integriteten, Vilken data anser ni skulle kunna vara mest känslig då isåfall? Är det samma eller skulle det skilja sig då?

(U)
Nej jag tror att det är samma. Allting som har med inloggningar och banker, det är där som det blir känsligt, för då kommer du åt så otrolig mycket information. Ja hemlarm om man ska ta det som exempel. Ja men då blir hela ett hus [...] utsatt, i och med om det blir inbrott till exempel. Men annars så är det ju egna enheten som mobiltelefonen, för där har man ju allting. All information ligger oftast där, alla konton, bankkonton, telefonböcker [...]. Det går att kartlägga ganska snabbt, om någon tar din telefon. Så nej, inte något speciellt som är extra känsligt än något annat.

(I)
Ja nu ska vi se, ja du nämnde just det här att användare oftast då inte byter lösenord och liknande och att det är en orsak till att till exempel identitetsstölder sker. Alltså hur kan man annars då som användare att förhindra att känslig information om en själv hamnar i fel händer, just inom det smarta smarta hemmet till exempel då?

(U)
Byta lösenord är ju jätteviktigt, se till så att det inte. Oftast har ju allting ett lösenord, som du ska in på, och ju klurigare och längre det är desto mer svårkläckt är det. Och så sen då, nej men inom familjen bör man väl sprida det, men att man liksom inte delar lösenord. Att varje person har sitt eget lösenord, och sen ja hur sparar man sitt lösenord? Egentligen är det inte bara det analoga steget att man har lösenord på en papperslapp, för den är ju svårare att hacka, för den finns ju inte ute på nätet. Då har du ju en massa papperslappar överallt då också. Så där finns ju appar som är liksom krypterade för svåra lösenord. Så att man hamnar i en ond cirkel, du måste ha lösenord för att komma åt lösenord. Och det är den problematiken du får dras med. Hur ska man göra ? Och det är hängslen och linan lite grann. Men återigen byta lösenord ofta på alla enheter, men folk är bekväma. Det är svårt att komma ihåg och hitta på nya lösenord och så blandar man och så ska man återställa. Men det är det viktigaste, ofta och långa och krångliga lösenord, då är man hyfsad säker.

(I)
Mm okej, men om man då ska till exempel köpa nya produkter, är det värt då att tänka på vad det är för företag som man köper utav, vad de säger med sina säkerhetspolicyer, eller om de har någon viss certifikat. Är det något man bör tänka på? När man liksom ska köpa in nya produkter?

(U)

Ja det beror ju på vad man ska köpa in och ser man till gemene man så är det ingen som läsa de här policyer eller villkoren och det blir för komplicerat och det blir för mycket jobb. Och sen då när man ska köpa något så ska man. Jag tror många rekar marknaden lite grann, men sen så söker man rätt pris. Sen kan man ju bara lita på vad företagen säger att de sparar, vad de har för policy. Och det är likadant i mitt arbete det är det enda man kan gå på. Det är vad dem säger, då får man ju, ja det är det som är trovärdigt. Man kan ju inte motbevisa det heller. Så att ja, samtidigt så beror det på vad man ska köpa, köper man en dator ja är det bättre med en HP eller Beats eller, ja det är jättesvårt att veta. Sen är det ju den informationen du lägger in på den. Det är den som du ansvarar för, sen om vad det är för slags enhet spelar inte så stor roll. Så ja, det är ju också så att alla är ju, ja men ett företag om du tar datorer till exempel, de är ju rädda om sitt rykte också, att inte de säger det för folk köper de produkterna så det är ingen som vill skriva någonting som de inte håller heller. För att kommer det ut läckor att ja men att företaget funkar inte, de läcker information, så det är ju en kan där också.

(I)
Mm precis, men brukar företag då, alltså ur eran synpunkt, samla in mer data än vad som behövs, alltså utifrån deras produkter och liknande?

(U)
Ja återigen det är, det är vad de skriver att de samlar in. Men sen vet man inte vad de använder det till. Å andra sidan när det gäller kommunikation så är jättemycket krypterad, så där ser de ingenting. Ändå vad som går sinsemellan, men ja. Basic information som man uppger själv absolut. Sen, det är ju också svårt att veta, men jag brukar vara lite misstänksam gentemot, ja när det gäller alla appar. Tar vi appar som exempel också, ja men de skriver att de samlar in [...] och klockslag och ingenting mer. Men där, beroende på vad det är för app så absolut, man samlar. För man vill ju marknadsföra, riktad reklam och så vidare. Så man har nog samlat in en hel del information.

(I)
Vad finns det för risker med att personlig data överförs mellan enheter, om det är någonting du känner till?

(U)
Förr tror jag att det var lättare, i och med att inte var så mycket var krypterat så var det lättare att fånga upp, både lösenord och konton och allting. Jag kan ju inte säga att det är helt säkert idag men det är ju mycket mycket säkrare idag när allting går krypterat, så då är det svårare att fånga upp information. Då måste du ju ID-kapa någon eller ja försöka liksom med väldigt avancerade verktyg och kunna hacka den här krypteringen och det gör man inte i första taget. Så absolut sen att man skickar känslig information eller mitt tyckte man att man har krypterat appar, eller mail,

man skickar inte lösenord och inloggningar på samma, för att man har, återigen, hängslen och livrem, så att de tar försiktighetsåtgärder för det också. Men som sagt, jag tror att det är svårare idag.

(I)
Mm, och sen vid intrång på nätverket, hur lång tid brukar det ta innan man, ja då på individnivå men även för ja företagen, upptäcker detta?

(U)
Oj, det där är ju så haha, ja företag har ju oftast en övervakning, de ser ju. De sitter och kollar vilken information som är på gång på deras nätverk, så de har ju verkligen hängslen och livrem så de ser ju till att stoppa det på en gång. Så där tror jag att det går rätt snabbt, men tidsspann är jättesvårt att säga. Men, där är man väldigt snabb för man villl skydda sin data, där har man programvaror för att larma och för att förhindra. Personligt däremot kan nog ta väldigt lång tid om en egentlig individ, innan den ska inse att den är hackad, datorn är hackad eller någonting. Eller att man har en skadlig kod eller någonting för det är ju inte alla som sitter med anitvirus heller, så då kan det ju ta ännu längre tid innan man förstår. Sen är det ju, jag menar antivirus är jätteviktigt att uppdatera, och uppdatera sitt operativsystem och sådär. Nej återigen, den här skadliga koden, den anpassar ju sig efter de här säkerhetskoden. Så där har du ju också ett mörkertal. Det är många som inte anmäler och det är även företag som inte heller anmäler även fastän de har blivit utsatta för att det är, ja dålig reklam för dem att de har blivit hackade, men det är ingenting man rår för själv så som företag, även fast man har tagit strid för och har beredskap och har programvaror för att förhindra.

(I)
Mm, när man då går från idé till realisering med smarta enheter som administrerar data, vad tycker du fokuser bör ligga? Är det då säkerhet eller till exempel effektivisering av vardagliga uppgifter?

(U)
Haha säkerheten, absolut.

(I)
Och sen om man kollar då, alltså från ert perspektiv, gör företagen tillräckligt, alltså tydliggör de tillräckligt mycket för individen och användarna av sina produkter, till exempel av smarta enheter i hemmet[...]. Gör företagen det tillräckligt tydligt för vad för data som behandlas?

(U)

Mm nja det där var, ja det där var lite klurigt. Nja, och det är upp till företagen. Jag menar återigen, vad de säger att de lagrar och inte lagrar. Sen beror det på vad det är för enheter man pratar om och vad det är för appar man använder. Många av enheterna man tar, ja smartphone eller nått där, den kommunicerar ju hela tiden. Det kollas in positionering och och det är ju, mer vad är den någonstans. Ska den hämta någon post, har det kommit några inlägg någonstans. Det kommuniceras ju hela tiden. Sen är det ju olika appar, de samlar ju säkert in olika information också.[...] Men ja det där var lite klurig fråga. Ja det är återigen upp till företagen.

(I)
Mm, men tror, tror du att de försöker göra det tydligt då, alltså så där, tror du de försöker göra det lätt för användarna att se vad för data som samlas?

(U)
Både och. Samtidigt så vill de ju få in så mycket information som möjligt om användaren. För att kunna rikta reklam och för att kunna anpassa appar och så vidare till personen i fråga. Samtidigt då när man installerar en app så godkänner man ju otroligt mycket access som den här appen ska få till din telefon. Jag tror inte det är många som tänker på det, men man släpper ju egentligen ifrån sig allting, du godkänner ju allt att den här appen ska ha åtkomst till rubbet på din telefon, då kan man inte komma i efterhand och säga någonting för du har liksom godkänt, vad heter det, user agreement. Så då har du ju godkänt att den här appen ska få full access, till bilder, kameror kontakter och så vidare och mycket mycket mycket mer. Ja då hamnar det på användaren. Och ska man som användare läsa igenom mycket mer noggrant vad man godkänner. Men godkänner man inte så kan man inte installera appen haha.

(I)
Haha nej men precis.

(U)
Så nog hämtar de in information, men beroende på vad vi pratar om, appar och datorer. Och smart hem, eller ja typ av hemlarmssystem, kanske inte har lika mycket dårå. Eller som en kaffebryggare, det är inte så mycket information som är viktig där då.

(I)
Mm men då, ur ert perspektiv, gör företagen tillräckligt för att tydliggöra för individen för vilka säkerhetsrisker som kan uppkomma vid användningen av tjänsterna?

(U)
Ja det beror på lite grann, ja det är också upp till företagen. Men jag tror att man måste tydliggöra det ganska mycket för om man ska få sin produkt såld. Beroende för vad det nu är för produkt.

Och liksom visa att det är, vi tänker på säkerhet och personlig integritet och så vidare för då blir ju ett förtroende gentemot, gemene man och så kan man då, så kommer man använda den här produkten. Vet man med sig att det har säkerhetshål eller att det är liksom läcker information, då blir ju inte det så populärt. Så ja, beroende på vad det är för någonting.

(I)
Yes, och om man tittar då på behörigheter, vid användning av enheter och appar och liknande. Är de viktiga ur både företagsperspektiv och kundperspektiv och isåfall varför eller varför inte?

(U)
Jo men det tycker jag. Som företagare att inte, de samlar ju in känslig information om individer. Och då ska ju inte alla ha tillgång till all information. Alla jobbar säkert inte med samma sak heller, det kan man se bland mitt jobb också. Det är att vissa får tillgång till viss information, alla får inte ha full access till all information som finns. [...] Arbetar man inte inom det området så behöver man inte ha en access gentemot den data heller. Så det är ju en trygghet både för personal som ja, eller anställda inom företag. Ju mindre du vet desto mindre kan du ju läcka också . Och då blir det en begränsad skara om man har koll vilka som accessar den informationen, Och det blir ju i sig också en trygghet för användaren. Om man nu som användare, många kanske inte bryr sig när man installerar en app, man tänker inte steget längre liksom men. Nej så det tror jag, eller är bra att ha begränsningar på vem som ser vad.

(I)
Mm, finns det något sätt som man alltså kontrollerar de här behörigheter då idag? Liksom, eller hur bör man tänkas kontrollera de här typerna av behörigheterna.

(U)
Som företagare till exempel, eller?

(I)
Ja.

(U)
Ja jo men då, då blir det att man loggar vem som går in och man har olika behörighetsnivåer och att allting loggas. Och även där kanske få någon larm om att ja men den här försöker accessa någonting som den inte är behörighet till. Så att man flaggar upp det ganska tydligt. Så att skadan inte redan är skedd, utan att man får en hint om innan att någon försöker göra något man inte är behörig till. Och det tror jag många företag eller och myndigheter, eller ja, jag tror det är ganska vanligt att man har det både på, ja allra helst inom myndigheter. För det är otroligt mycket

information som finns inom systemen som folk inte ska ta reda på vad det är för något. Eller ta del utav.

(I)
Och sen just tillgänglighet av data, som användare och som privatpersoner i då till exempel ja men hemmet, är tillgänglighet av dessa data viktig då för användaren och privatpersonen?

(U)
Nej det tycker jag inte att du som användare, eller ska ha rätt till. Det är klart att du ska få ut din information men du ska själv inte kunna komma åt den information. För då vet man ju inte vad för mer information kring information man kan komma åt, och får ta del av. Och återigen, det är ju företagen som äger den informationen, så vill man ha ut sin egen information om just sitt hemlarm, ja men då får man kontakta företaget, så får man ut den informationen, som de anser inte är sekretess och som du som ja individ kan få ta del av. Sen om det är all information, det vet man ju inte.

(I)
Mm, du säger då typ att företagen då har rätt till, äger den informationen. Är det så det brukar ligga till vid användning av olika typer av enheter [...] att det är företagen som faktiskt äger rätten till den data som ligger lagrad om mig i enheterna?

(U)
Ja mycket på sociala medier och ja, men när du skapar egna bloggar och v-bloggar och sånt där. Då godkänner man ju, du lagrar ju information någonstans. Sen visst så de har ju krypterat, men det som är öppet går mycket till företagen, att de får rätt till att använda den informationen, de bilder som du sparade. Så att ja.

(I)
Vad heter det, nu men GDPR som kommer sättas i verket i Maj, kommer det hjälpa till tror du, i skyddandet av den personliga integriteten ur användarens perspektiv?

(U)
Jag tror det, eller joo men det tror jag att, den är ju till för användarna för att säkra att informationen skyddas mer. Så att jag tror absolut att folk kanske mer förstår begreppet av all data som man slänger omkring sig till höger och vänster och liksom lite grann vet att säkerhetstänket på ett annat perspektiv så att folk tänker till lite mer. Så absolut tror jag har mer nytta att det har kommit upp i dagsljuset mer, så att folk förstår lite grann mer och får lite mer insikt i vad är det som händer när man ändå använder internet. För jag vet att många tänker inte på det. Man bara använder det, det bara finns där och man skickar information hit och dit utan att

tänka på vidare konsekvenser av den informationen. Så absolut så tror jag det är jättebra att det har blivit en reminder och lite omstrukturering av den. Absolut.

(I)
Okej. [...] Men då är vi jättenöjda.

(U)
Fick ni svar på några frågor? Haha.

(I)
Haha jodå vi fick svar på jättemycket. Så tack så jättemycket för att du tog dig tiden.

8. Referenser

Agarwal, A. & Agarwal, A. (2011). The Security Risks Associated with Cloud Computing, *Journal of Computer Applications in Engineering Sciences*, vol. 1 (Special Issue on CNS), pp. 257-259, Tillgänglig Online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.207.9119&rep=rep1&type=pdf [Hämtad 2018-04-11]

Ali-ud-din Khan, M., Uddin, M.F. & Gupta, N. (2014). Seven V's of Big Data Understanding Big Data to extract Value, *Proceedings of 2014 Zone 1 Conference of the American Society for Engineering Education* (ASEE Zone 1), IEEE, pp. 1-5, Tillgänglig Online: http://asee-ne.org/proceedings/2014/Professional%20Papers/113.pdf [Hämtad 2018-04-15]

Amazon. (2017). Introducing the Next Generation of Echo: the All-New Amazon Echo and Echo Plus, Tillgänglig Online: http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=2303270 [Hämtad 2018-04-09]

Anandarajan, M. & Simmers, C.A. (2018). The Internet of People, Things and Services: Workplace Transformations (Routledge Studies in Employment Relations), Tillgänglig Online: https://books.google.se/books?hl=sv&lr=&id=ORdSDwAAQBAJ&oi=fnd&pg=PT242&dq=%22IoT+security+triad%22&ots=jJSEpmEBFk&sig=Atbu3WezNFRo0MNrG77kFDW5zPw&redir_esc=y#v=onepage&q=%22IoT%20security%20triad%22&f=true [Hämtad 2018-04-11]

Apple. (2014). Apple Releases iOS 8 SDK With Over 4,000 New APIs, Available Online: https://www.apple.com/newsroom/2014/06/02Apple-Releases-iOS-8-SDK-With-Over-4-000-New-APIs/ [Hämtad 2018-04-09]

Apple. (2018). Privacy Policy, Available Online: https://www.apple.com/legal/privacy/en-ww/ [Hämtad 2018-04-28]

Ashton, K. (2009). That 'Internet of Things' Thing, *RFID Journal*, 22 Juni, Tillgänglig Online: http://www.rfidjournal.com/articles/view?4986 [Hämtad 2018-04-16]

Atanassov, K.T., Kacprzyk, J., Kałuszko, A., Krawczak, M., Owsiński, J., Sotirov, S., Sotirova, E., Szmidt, E., Zadrożny, S., (eds). (2016). Uncertainty and Imprecision in Decision Making and Decision Support: Cross-Fertilization, New Models and Applications, Tillgänglig Online: https://books.google.es/books?id=FM44DwAAQBAJ&pg=PA306&lpg=PA306&dq=characterist

ics+of+big+data+valence&source=bl&ots=wt7Gh15YCC&sig=F9dSuMLyS2qg-vw092t8brAR1xs&hl=en&sa=X&ved=0ahUKEwjV_9yMj7DaAhXMPxQKHRHkBtU4ChDoAQhCMAU#v=onepage&q=characteristics%20of%20big%20data%20valence&f=false [Hämtad 2018-04-15]

Aziza, B. (2018). Facebook Privacy Scandal Hearings: What You Missed, *Forbes*, 16 April, Tillgänglig Online: https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/ciocentral/2018/04/16/facebook-privacy-scandal-hearings-what-you-missed/&refURL=&referrer=#263f74e87ab9 [Hämtad 2018-04-17]

Balebako, R., Faith Cranow, L., Jung, J., Lu, W. & Nguyen, C. (2013). "Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones, Tillgänglig Online: https://cups.cs.cmu.edu/soups/2013/proceedings/a12_Balebako.pdf [Hämtad 2018-04-27]

Bigelow, S.J. & Rouse, M. (2016). Big Data, *TechTarget*, 16 Maj, Tillgänglig Online: https://searchdatamanagement.techtarget.com/definition/big-data [Hämtad 2018-04-15]

Birchley, G., Huxtable, R., Murtagh, M., ter Meulen, R., Flach, P., & Gooberman-Hill, R. (2017). Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. *BMC Medical Ethics*, Tillgänglig Online: http://doi.org/10.1186/s12910-017-0183-z [Hämtad 2018-04-09]

Blake-Plock, S. (2017). Where's The Value In Big Data?, *Forbes*, 14 April, Tillgänglig Online: https://www.forbes.com/sites/forbestechcouncil/2017/04/14/wheres-the-value-in-big-data/#6397e4fc30da [Hämtad 2018-04-16]

Botta, A., Donato, W., Persico, V. & Pescapè, A. (2014). On the integration of cloud computing and internet of things. *Proceedings of the 2014 International Conference on Future Internet of Things and Cloud*, pp. 23-30, Tillgänglig Online: https://pdfs.semanticscholar.org/9886/62b9759adb01ae9fd2e219c435a66e1488e5.pdf [Hämtad 2018-04-19]

Bugeja, J., Jacobsson, A. & Davidsson, P. (2016). On Privacy and Security Challenges in Smart Connected Homes, *Proceedings of the 2016 European Intelligence and Security Informatics Conference*, pp. 172-175, Tillgänglig Online: https://muep.mau.se/bitstream/handle/2043/21507/2857a172.pdf?sequence=4 [Hämtad 2018-04-05]

Bui, Y.N. (2009). How to Write a Master's Thesis, London, UK: Sage Publications Ltd.

CompterSweden (2018). Big Data, Tillgänglig Online: https://it-ord.idg.se/ord/big-data/ [Hämtad 2018-04-11]

Datainspektionen (2012). *Inbyggd Integritet - Privacy by design – Inbyggda mekanismer i IT-system för skydd av den personliga integriteten*, Tillgänglig Online: https://www.datainspektionen.se/Documents/faktablad-inbyggd-integritet.pdf [Hämtad 2018-04-05]

Datainspektionen (2017a). *Känsliga personuppgifter, uppgifter om brott och personnummer Känsliga personuppgifter, uppgifter om brott och personnummer*, Tillgänglig Online: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/kansliga-personuppgifter-uppgifter-om-brott-och-personnummer/ [Hämtad 2018-04-05]

Datainspektionen (2017b). *Dataskyddsförordningen - General Data Protection Regulation (GDPR)*, Tillgänglig Online: https://www.datainspektionen.se/Documents/Dataskyddsf%C3%B6rordningen%20-%20Datainspektionen.pdf [Hämtad 2018-04-05]

Dumbill, E. (2012). Volume, Velocity, Variety: What You Need to Know About Big Data, *Forbes*, 19 Januari, Tillgänglig Online: https://www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/#23dd3c311b6d [Hämtad 2018-04-15]

EC-Council (n.d.). Certified Ethical Hacker Certification, Tilgänglig Online: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ [Hämtad 018-05-05]

Eastwood, G. (2017). How to bring data analytics into the smart home infrastructure, *NetworkWorld from IDG*, 18 Juli, Tillgänglig Online: https://www.networkworld.com/article/3208748/emerging-technology/how-to-bring-data-analytics-into-the-smart-home-infrastructure.html [Hämtad 2018-04-16]

Evans, D.L., Bond, P.J. & Bement, A.L. (2004). Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199), Gaithersburg, Tillgänglig Online: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf [Hämtad 2018-04-11]

Farooq, M.U., Waseem, M., Khairi, A. & Mazhar, S. (2015) A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1-6, Tillgänglig Online: https://doi.org/10.5120/19547-1280 [Hämtad 2018-04-11]

Friedman, A. & Singer, P.W. (2014). What Do We Mean By Security Anyway?, Tillgänglig Online: https://www.brookings.edu/opinions/what-do-we-mean-by-security-anyway/ [Hämtad 2018-04-15]

Ghosh, K. & Nath, A. (2016). Big Data: Security Issues and Challenges, *International Journal of Research Studies in Computer Science and Engineering*(IJRCSE), vol. 3, no. 3, pp. 1-9, Tillgänglig Online: https://www.researchgate.net/publication/304624841_Big_Data_Security_Issues_and_Challenges [Hämtad 2018-04-15]

Hendersen, A. (2017). The CIA Triad: Confidentiality, Integrity, Availability, Tillgänglig Online: http://panmore.com/the-cia-triad-confidentiality-integrity-availability [Hämtad 2018-04-11]

Hendricks, D. (2014). The History of Smart Homes, *IoT Evoloution - M2M Feature News*, 22 April, Tillgänglig Online: http://www.iotevolutionworld.com/m2m/articles/376816-history-smart-homes.htm [Hämtad 2018-04-05]

IBM. (2018). CIA "Triad", Tillgänglig Online: https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/ [Hämtad 2018-05-10]

Informatica (n.d.). What is Data Analytics?, Tillgänglig Online: https://www.informatica.com/services-and-training/glossary-of-terms/data-analytics-definition.html#fbid=RO_BpPQks5p [Hämtad 2018-04-16]

Investopedia. (2017). Internet of Things (IoT), Tillgänglig Online: https://www.investopedia.com/terms/i/internet-things.asp [Hämtad 2018-04-16]

Investopedia. (2018a). Cloud Computing, Tillgänglig Online: https://www.investopedia.com/terms/c/cloud-computing.asp [Hämtad 2018-04-10]

Investopedia. (2018b). Smart Home, Tillgänglig Online: https://www.investopedia.com/terms/s/smart-home.asp [Hämtad 2018-04-10]

Jacobsen, D. I. (2002). Vad, hur och varför : om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen, Lund : Studentlitteratur.

Bui, Y.N. (2009). How to Write a Master's Thesis, London, UK: Sage Publications Ltd.

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system, *Future generations computer systems*, vol. 56, pp. 719–733, Tillgänglig Online: https://doi.org/10.1016/j.future.2015.09.003 [Hämtad 2018-04-09]

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. *Proceedings in 10th International Conference on Frontiers of Information Technology (FIT)*, pp. 257-260, Institute of Electrical and Electronics Engineers Inc, Tillgänglig Online: https://pure.qub.ac.uk/portal/files/81384964/PID2566391.pdf [Hämtad 2018-04-16]

Kovach, S. (2015). There's actually a strong case for connecting everything in your home to the internet, *Business Insider*, 28 Juni, Tillgänglig Online: http://www.businessinsider.com/why-you-might-want-a-smart-home-2015-6?r=US&IR=T&IR=T [Hämtad 2018-04-19]

Laney, D. (2001). 3D data management: Controlling data volume, velocity, and variety. Application Delivery Strategies, Metagroup, Tillgänglig Online: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf [Hämtad 2018-04-15]

Leuschner, P. (2017). How data analytics is adding value in the smart home, *Smart Cities Dive*, 6 Juli, Tillgänglig Online: https://www.smartcitiesdive.com/news/how-data-analytics-is-adding-value-in-the-smart-home/446406/ [Hämtad 2018-04-16]

Mair, C. (2018). The challenges and opportunities of data sharing across complex industrial value chains, Tillgänglig Online: https://www.sirris.be/agenda/challenges-and-opportunities-data-sharing-across-complex-industrial-value-chains [Hämtad 2018-05-02]

MarketsandMarkets. (2017). Smart Home Market worth 137.91 Billion USD by 2023, Tillgänglig Online: https://www.marketsandmarkets.com/PressReleases/global-smart-homes-market.asp [Hämtad 2018-04-09]

Mell, P and Grance, T. (2011). The NIST Definition of Cloud Computing. NIST, USA. Tillgänglig Online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Hämtad 2018-04-19]

Metivier, B. (2017). Fundamental Objectives of Information Security: The CIA Triad, web blog post tillgänglig online: https://www.sagedatasecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad [Hämtad 2018-04-11]

Mendes, T.D.P., Godina, R., Rodrigues, E.M.G., Matias, J.C.O. & Catalao, J.P.S. (2015). Smart home communication technologies and applications: Wireless protocol assessment for home area network resources, *Energies*, *8*, 7279-7311, Tillgänglig Online: http://www.mdpi.com/1996-1073/8/7/7279/htm [Hämtad 2018-04-05]

Mertens, D.M., Hesse-Biber, S. (2012). Triangulation and Mixed Methods Research: Provocative Positions, *Journal of Mixed Methods Research*, vol. 6, no. 2, pp. 75-79, Tillgänglig Online: http://journals.sagepub.com/doi/pdf/10.1177/1558689812437100 [Hämtad 2018-04-20]

Microsoft Azure (n.d.a) What is Cloud computing? Tillgänglig Online: https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/ [Hämtad 2018-04-23]

Microsoft Azure (n.d.b) What is the Cloud? Tillgänglig Online: https://azure.microsoft.com/en-us/overview/what-is-the-cloud/ [Hämtad 2018-04-23]

Molina-Markham, A., Prashant, S., Fu, K., Cecchet, E., & Irwin, D. (2010). Private Memoirs of a Smart Meter, *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-efficiency in Building*, pp. 61-66, Tillgänglig Online: https://spqr.eecs.umich.edu/papers/molina-markham-buildsys10.pdf [Hämtad 2018-04-05]

Morgan, J. (2014). A Simple Explanation Of 'The Internet Of Things', *Forbes*, 13 Maj, Tillgänglig Online: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#c42041c1d091 [Hämtad 2018-04-09]

National Academy of Engineering. (2018). Household appliances timeline, Tillgänglig Online: http://www.greatachievements.org/?id=3768 [Hämtad 2018-04-09]

Norton. (2018). The Connected Home: How Safe is it?, Tillgänglig Online: https://us.norton.com/internetsecurity-iot-the-connected-home-how-safe-is-it.html [Hämtad 2018-04-09]

Olsdotter-Arnmar, A. & Näslund, L. (2013). Storbedragaren som hjälper polisen, *SVT Nyheter*, 10 Oktober, Tillgänglig Online: https://www.svt.se/kultur/storbedragaren-som-blev-fbi-anstalld-pa-sverige-besok [Hämtad 2018-04-14]

Perwej, Y. (2017). An Experiential Study of the Big Data, *International Transaction of Electrical and Computer Engineers System*, vol. 4, no. 1, pp. 14-25, Tillgänglig Online: http://pubs.sciepub.com/iteces/4/1/3/ [Hämtad 2018-04-15]

Quah, A.M.Y. & Röhm, U. (2013). User Awareness and Policy Compliance of Data Privacy in Cloud Computing, *Proceedings of the First Australasian Web Conference* (AWC 2013), vol. 144, pp. 3-12, Adelaide, Australia, Tillgänglig Online: https://pdfs.semanticscholar.org/bd87/4ec85f323d1d05c209eeee10fde61d8eb065.pdf [Hämtad 2018-05-02]

Robinson, R. (2018). Data Privacy vs. Data Protection, web blog post tillgänglig online: https://blog.ipswitch.com/data-privacy-vs-data-protection [Hämtad 2018-04-11]

Samsung. (2014). Samsung Smart Home Becomes Reality, Set To Transform Everyday Life, Tillgänglig Online: https://news.samsung.com/global/samsung-smart-home-becomes-reality-set-to-transform-everyday-life [Hämtad 2018-04-09]

Samsung (n.d.). Family hub - hemmets nya mittpunkt, Tillgänglig Online: http://www.samsung.com/se/refrigerators/french-door-rf56m9540sr/ [Hämtad 2018-05-16]

SAS (n.d.). Big Data- What is it and why it matters?, Tillgänglig Online: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html [Hämtad 2018-05-16]

Sethi, P. & Sarangi, S.R. (2017). Internet of Things: Architectures, Protocols, and Applications, *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 9324035, 25 pages, Tillgänglig Online: https://doi.org/10.1155/2017/9324035 [Hämtad 2018-04-16]

Statista (2018a). Volume of data collected by smart buildings worldwide from 2010 to 2020 (in zetabytes), Tillgänglig Online: https://www.statista.com/statistics/631151/worldwide-data-collected-by-smart-buildings/ [Hämtad 2018-04-09]

Statista (2018b). Smart Home, Tillgänglig Online: https://www.statista.com/outlook/279/100/smart-home/worldwide# [Hämtad 2018-04-09]

Statistiska Centralbyrån (2018). Frågeteknik, Tillgänglig Online: http://www.scb.se/dokumentation/statistikguiden/undersokning-och-urval/frageteknik/ [Hämtad 2018-05-05]

Svenska Akademins Ordlista (n.d.). Plagiera, Tillgänglig Online: http://www.saob.se/artikel/?seek=plagiera [Hämtad 2018-04-16]

Techopedia (n.d.). Cyclic Redundancy Check (CRC), Tillgänglig Online: https://www.techopedia.com/definition/1793/cyclic-redundancy-check-crc [Hämtad 2018-04-17]

W3Schools (n.d.). Introduction to SQL, Tillgänglig Online: https://www.w3schools.com/sql/sql_intro.asp [Hämtad 2018-04-16]

Lagar & Regler

Dir. 2014:65 Den Personliga Integriteten, Tillgänglig Online: https://www.riksdagen.se/sv/dokument-lagar/dokument/kommittedirektiv/den-personliga-integriteten_H2B165 [Hämtad 2018-04-11]

SFS 1998:204. *Personuppgiftslagen*. Stockholm: Justitiedepartementet, Tillgänglig Online: https://lagen.nu/1998:204 [Hämtad 2018-04-11]

SOU 2017:52. Så stärker vi den Personliga Integriteten, Stockholm: Integritetskommittén, Tillgänglig Online: http://www.regeringen.se/4ac6ee/contentassets/56e701d354824bcb9826ea0839ab28f3/sa-starker-vi-den-personliga-integriteten-sou-201752 [Hämtad 2018-04-11]