«Hei, Google! Overvåker du meg?»

Smarthøyttalere, personvern og overvåking:
Hva tenker forbrukerne?

Emma Louise Fon Mathisen

Masteroppgave i medier og kommunikasjon

Institutt for informasjons- og medievitenskap

Våren 2021

Forord

Jeg hadde aldri sett for meg at jeg skulle skrive min masteroppgave midt under en global pandemi. Det er ikke til å legge skjul på at det har vært krevende, frustrerende og ensomt til tider. Likevel har det vært en lærerik og givende prosess. Det å skrive masteroppgave hjemmefra har lært meg viktigheten av selvdisiplin, rutiner og ikke minst det å ta pauser og koble av med god samvittighet. Til syvende og sist har dette året gitt meg erfaringer jeg ikke ville vært foruten.

Det er mange mennesker som fortjener en takk i forbindelse med min masteroppgave. Jeg hadde ikke klart å holde motivasjonen oppe om det ikke hadde vært for dere.

Aller først vil jeg si tusen takk til min veileder Knut Helland. Dine gode råd, ditt engasjement og ikke minst din tilgjengelighet har gjort til at jeg nå kan levere fra meg et prosjekt jeg er stolt av. Til tross for utfordringer og frustrasjon underveis har det stort sett vært en fornøyelse å skrive masteroppgave. Din veiledning har gjort at jeg har sluppet unna skippertaksarbeid, stress og søvnløse netter, og for det er jeg evig takknemlig.

Jeg vil også rette en stor takk til min familie, og særlig mine to søstre, Inger Elisabeth og Vilde Amalie. Takk for at dere alltid er der når jeg trenger hjelp, motiverende ord, eller bare trenger å få ut litt frustrasjon. En ekstra takk til min søster Vilde Amalie, og min venninne Thea Kristin, som hjalp meg å komme i kontakt med informanter i USA.

En spesiell takk til min gode venninne Oda Eline, som har hjulpet meg med korrekturlesing. Tusen takk for at du alltid stiller opp og er der for meg.

Sist men ikke minst ønsker jeg å rette en stor takk til hver eneste informant. Deres tid, engasjement og bidrag har vært uvurderlig. Dette prosjektet hadde ikke blitt til uten dere.

Sammendrag

Formålet med denne masteroppgaven har vært å undersøke hvordan unge mennesker i Norge og USA reflekterer rundt overvåking og personvern i bruken av smarthøyttalere. De populære enhetene med en alltid-lyttende mikrofon har tidligere blitt kritisert for å være en trussel mot personvernet, og en måte for store selskaper å samle inn enorme mengder data fra sine forbrukere. Derfor har jeg i min masteroppgave undersøkt forbrukeres bevissthet rundt kommersiell overvåking, og deres syn på personvern.

Jeg har valgt å gjøre en komparativ studie med både norske og amerikanske informanter. Dette vil kunne kartlegge om forbrukere av samme teknologi forhandler om sine persondata med samme bevissthet, på tvers av kultur. De to ledende aktørene innen smarthøyttalere, Google og Amazon, dominerer hvert sitt marked. Amazon dominerer det amerikanske markedet, og Google dominerer det norske. Gjennom 11 kvalitative intervjuer har jeg fått en forståelse av hvordan norske og amerikanske forbrukere reflekterer rundt eget personvern og overvåkingskapitalisme, og hvordan de håndterer sine bekymringer omkring dette i praksis.

Resultatene viser at de norske informantene i større grad har en kritisk holdning til informasjonsinnhenting og målrettet reklame i bruken av smarthøyttalere, sammenliknet med de amerikanske. I tillegg er de norske informantene bevisste på hvilken stemme de ønsker at smarthøyttalerens assistent skal ha. De norske informantene foretrekker en assistent med kvinnelig stemme, og dette er basert på trygghet av kvinner, og stereotypiske kjønnsroller av menn. Valget rundt assistentens stemme er ikke vektlagt hos de amerikanske informantene, og de har et generelt mer avslappet forhold til bruken av smarthøyttalere.

Til tross for at det er de norske informantene som i størst grad reflekterer rundt personvern og overvåking i bruken av smarthøyttalere, ser det ut til å være en manglende forståelse for kommersiell overvåking, både hos de norske og amerikanske informantene. Personvern er noe som blir ansett som viktig av de fleste, men de færreste tar aktive grep for å beskytte personlig informasjon.

Innholdsfortegnelse

1. Innledning

«Få sjekket den kulen! Ta en klemmedag i måneden der du sjekker dyret ditt for kuler og forandringer».

Dette var annonsen jeg fikk i mine sosiale medier etter en telefonsamtale med min søster. Ikke en oppsiktsvekkende annonse i seg selv. Men saken er den at jeg ikke har noe kjæledyr, og jeg har derfor ikke søkt etter svulster hos hunder på internett. Likevel var det neppe tilfeldig at akkurat denne annonsen skulle pryde mine sosiale medier i flere dager. Min søster ringte meg nemlig for å fortelle at *hun* hadde oppdaget en kul i hoften til sin nylig adopterte hund. Det var altså tydelig at min private telefonsamtale var blitt lyttet til og forsøkt brukt på en kommersiell måte. Dermed fikk en helt ordinær telefonsamtale en uhyggelig bismak av overvåking og innblanding, og hvis jeg ikke har søkt på svulster hos hunder på internett, hvordan ble da samtalen registrert?

Jeg tok en vurdering av tingene rundt meg med integrert mikrofon, i tilfelle det var slik samtalen var tatt opp. Mobiltelefonen min er selvsagt en mulig og sannsynlig kandidat. Det var jo denne jeg snakket i. Kanskje telefonens integrerte assistent, Siri, fikk med seg samtalen, og trodde jeg gjorde et internettsøk. I tillegg til telefonen var det også en smarthøyttaler i rommet. Kan smarthøyttalerens mikrofon ha fått med seg samtalen og solgt den videre?

Jeg fikk min smarthøyttaler, en Google Home, i gave. Jeg koblet høyttaleren opp uten å egentlig tenke over hvem jeg ga tilgang til innsiden av hjemmet mitt. Hadde et selskap som Google spurt om de kunne få plassere en mikrofon i hjemmet mitt, ville jeg sannsynligvis himlet med øynene og sagt nei før de rakk å fullføre setningen. Men Google forkledd som en vennlig, kvinnelig «assistent» gjorde meg tydeligvis ingenting. Og jeg trivdes den første tiden med Google som romkamerat. Jeg kunne for eksempel be assistenten minne meg på middagen i ovnen, eller sette på TV for meg. Likevel varte ikke denne utopiske nye hverdagen så veldig lenge. Plutselig begynte assistenten å svare på spørsmål som aldri var stilt. Til å være en som ser litt for mye på skrekkfilm, var det uhyggelig å våkne av en stemme midt på natten som sa «beklager, jeg hørte ikke hva du sa. Kan du gjenta spørsmålet?». Da jeg i tillegg fikk annonser som tilsynelatende var basert på samtaler, og ikke internettsøk, ble jeg plutselig usikker på hva den fikk med seg og ikke.

Jeg ble overrasket over min tidligere ukritiske holdning til teknologi som evner å samle inn informasjon om hvem jeg er i mitt eget hjem. I motsetning til en mobiltelefon som kan ringe, sende sms, ta bilder, og holde kontakten med andre mennesker, kunne assistenten i mitt tilfelle kun gjennomføre svært enkelte oppgaver. Oppgaver som jeg like gjerne kunne gjort selv. Det virket som om jeg potensielt ga bort veldig mye informasjon om meg selv, uten å få noe spesielt verdifullt tilbake.

Aksepten jeg hadde til å slippe et gigant-selskap som Google rett inn på soverommet mitt, ga meg en idé til masteroppgaven min. Hvilke tanker og refleksjoner har egentlig unge mennesker om overvåking og personvern når det gjelder smarthøyttalere?

Denne masteroppgaven vil derfor se nærmere på forholdet mellom forbruker og smarthøyttaler. Ikke fordi jeg tror smarthøyttalere nødvendigvis er det avgjørende elementet i overvåkingskapitalisme, eller personvernbrudd. Jeg har valgt å fokusere på smarthøyttalere fordi jeg mener det kan sees på som et slags symbol på den normaliserte aksepten til å invitere overvåkingen inn på et mer personlig plan. I mitt tilfelle ville jeg aldri sagt ja til å ha en mikrofon i hjemmet mitt, men en mikrofon integrert i en høyttaler med en vennlig, kvinnelig stemme gjorde at all skepsis forsvant. Derfor vil jeg undersøke hvorvidt forbrukere tar et informert valg når de plasserer en slik assistent i hjemmene sine, og hvordan de håndterer og aksepterer personvernsutfordringene en slik enhet fører med seg.

1.1. Tema og bakgrunn

Smarthøyttalere med sine intelligente personlige assistenter (heretter kalt IPA), bygger på et system som evner å lære av forbrukerens oppførsel og interesser. Dette gjør at assistenten kan kommunisere og respondere deretter (Manikoda, 2018). En IPA er utstyrt med en alltid-lyttende mikrofon, og blir aktivert når forbrukeren sier aktiveringsordet, som for eksempel «Alexa» eller «Hei, Google». Disse systemene som alltid lytter i bakgrunnen blir allestedsnærværende, og til tross for de mange personvernutfordringene som en IPA har, fortsetter populariteten å øke kontinuerlig (Manikoda, 2018). I 2019 var det anslått å være omtrent 3.25 milliarder IPAer i bruk på verdensbasis. Innen 2023 er det estimerte tallet hele 8 milliarder enheter, et tall høyere enn verdens befolkning (Tanovska, 2020). Da Google lanserte sin IPA i europeiske land som Norge, Sverige, Danmark og Nederland høsten 2018, var det et tydelig grep fra Googles side om å bli mer tilstedeværende gjennom Europa. To år

tidligere ble Google Home og Amazon Echo lansert i Storbritannia og Tyskland, og enda to år tidligere ble Amazon Echo først lansert i USA (Pridmore, et al., 2019).

Noen av de største teknologi-selskapene i verden, som Google og Amazon, har blitt våre nye romkamerater. Deres hensikt er tilsynelatende å gjøre hverdagen vår lettere, og hjemmet vårt smart. Innenfor hjemmet kan IPA ta form som for eksempel lydplanker og spillkonsoller, og ikke minst de populære smarthøyttalerne (Malkin, 2019). Amazon Echo med deres assistent Alexa, og Google Home med sin Google Assistant, er to av de største selskapene som har erkjent at en IPA ikke bare fungerer som en inngangsport til hjemmet, men også som et viktig kontrollsenter i smart-hjemmets økosystem (Ali & Yusuf, 2018).

1.2. Problemstilling

Google Home ble en del av min hverdag, og jeg tenkte aldri på hva som skjedde med dataen som ble samlet inn. Etter flere måneders bruk ble jeg gjort oppmerksom på at alle samtaler mellom meg og min IPA ble lagret permanent. Det føltes ikke som verdens undergang, men likevel ikke helt greit. Det var vanskelig å forstå hensikten med at Google skulle ha så mange lydopptak fra min helt alminnelige hverdag. Jeg oppfattet det i hvert fall ikke som en funksjon som skulle være til min fordel. Etter flere ubehagelig opplevelser valgte jeg å koble den ut. Det føltes som at den tok mer enn den ga i retur.

Amazon og Google er de største leverandørene på det vestlige markedet innen IPA. Amazon dominerer det amerikanske markedet, der hele 20% av den voksne befolkningen benytter seg av dette systemet (Buchholz, 2021). Google er den eneste at de to ovennevnte leverandørene som i dag tilbyr assistenten på norsk, og er per dags dato ledende på det skandinaviske markedet (hifiklubben, u.å). Derfor har jeg valgt å undersøke problemstillingen fra et internasjonalt perspektiv, med norske og amerikanske informanter. På denne måten kan jeg inkludere begge leverandører, som er ledende på hvert sitt marked. I tillegg har de to selskapene tilsynelatende ulike motiver/formål med å hente inn data/lagre data fra sine forbrukere. Mens Amazons fokus på datainnsamling ser ut til å være for å øke personlig salg på tvers av deres shoppingplattform, er Google avhengig av sin overvåkingsinfrastruktur for å videreutvikle den AI-drevne annonseringsplattformen deres (Pridmore, et al., 2019). Dermed kan en internasjonal tilnærming kartlegge om kulturelle forskjeller, personvernforordningen

GDPR, eller IPA-markedet i de forskjellige landene, har en innvirkning på unge brukeres forståelse og forhandlinger rundt personvern og overvåking i bruken av IPA.

Studiens problemstilling er som følger:

> *Hvilke refleksjoner har brukere av intelligente personlig assistenter rundt personvern og overvåking?*

Problemstillingen har jeg valgt å løse ved hjelp av fire analytiske dimensjoner. Disse vil jeg redegjøre for nå.

1.3. Analytiske dimensjoner

De analytiske dimensjonene belyser på hver sin måte viktige perspektiver knyttet til overvåking og personvern i bruken av IPA. Dimensjonene vil bli belyst gjennom hvert sitt kapittel, hvor jeg presenterer analytiske funn med en gjennomgående diskusjon. Med en problemstilling som undersøker forbrukerperspektivet, er det viktig at dimensjonene fungerer som et verktøy for å besvare selve problemstillingen. Dimensjonene er utarbeidet basert på teori, tilnærmingsperspektiver, hva som er relevant å diskutere fra en forbrukers perspektiv, og hva som vekket mest engasjement i pilotstudiene. Kapitlene bygger på hverandre, og til tross for at de belyser ulike temaer, fungerer de som viktige støttespillere for hverandre. Til sammen skaper de et helhetlig bilde av forbrukeres tanker, refleksjoner og mulig bekymringer i bruken av IPA. Fremfor alt belyser de fire dimensjonene de viktigste aspektene i problemstillingen, samtidig som de er grunnlag for gjennomføringen av analyse.

1.3.1. Overvåking

Overvåking er studiens første analytiske dimensjon, og inngang til den empiriske analysen. Ettersom informantene har valgt å plassere en IPA med en alltid-lyttende mikrofon i hjemmet sitt, er deres refleksjoner til fenomenet overvåking relevant. Dette kapittelet er basert på overvåkingsteori som inkluderer bl.a. Michel Foucaults panoptikon-konsept, og Shoshana Zuboffs teori om overvåkingskapitalisme.

1.3.2. Personvern

Personvern er studiens andre analytiske dimensjon. Personvernutfordringer i forbindelse med IPA har vært mye omdiskutert, og i 2018 advarte forbrukerrådet mot Googles IPA (Drabløs, 2018). Personvern er en naturlig oppfølging fra den foregående dimensjonen, og særlig viktig ettersom Norge og USA har ulike lover hva gjelder datainnsamling. Kapittelet bygger på personvernteorien til James H. Moor, i tillegg til Helen Nissenbaums teori om kontekstuell integritet. Dimensjonen vil belyse informantenes holdninger til eget personvern, og hvorvidt de har tillitt til at IPAens leverandør håndterer deres persondata i tråd med deres forventinger.

1.3.3. Påvirkning

De fleste selskaper er åpne om at de benytter forbrukerdata til markedsføringsformål, og dette vil enkeltpersoner oppleve i form av målrettede annonser. Innsamling av forbrukerdata foregår ofte gjennom informasjonskapsler, mikrofoner, eller andre tillatelser forbrukeren gir selskapet. Derfor vil holdninger til påvirkning trolig ha en sammenheng mellom informantenes holdninger til eget personvern. Dimensjonen bygger på Zuboffs teori om overvåkingskapitalisme, og utforsker informantenes holdninger til personlig målrettet reklame, og hvorvidt de føler de blir påvirket.

1.3.4. Menneskelig egenskaper (Antropomorfisme)

Studiens siste analytiske dimensjon bygger på antropomorfisme, som betyr å tilegne menneskelige egenskaper til ikke-menneskelige ting eller vesener (Haugen, 2019). IPA er ofte utviklet med en kvinnelig stemme, og i mange tilfeller et kvinnelig navn. Dette er for å gjøre forbrukeren mer komfortabel med å ha et stort selskap som Google og Amazon plassert i hjemmet med en tilkoblet mikrofon (Woods, 2018). Google tilbyr mannlig stemme, men det gjør ikke Amazon gjør per dags dato (hifiklubben). Stereotypiske kjønnsroller, hvor kvinnen blir sett på som en omsorgsperson, eksempelvis en mor eller kone, har vært viktig i utviklingen av IPA. Denne dimensjonen undersøker derfor hva informantene mener om IPAens menneskelig egenskaper, og hvorvidt kvinnelig fremtoning er det foretrukne valget hos informantene.

1.4. Begrepsavklaring

Enkelte begreper er gjennomgående i studien, og jeg vil nå kort redegjøre for hvordan jeg benytter meg av ulike begreper.

1.4.1. Intelligente personlig assistenter (IPA)

Intelligente personlig assistenter (forkortelse IPA) går under mange navn. Smarthøyttalere, smart-assistenter, personlig assistenter, Echo, Google Home, og mange bruker kun navnet til assistenten, som for eksempel Alexa. For å holde språket konsekvent gjennom studien, har jeg valgt å bruke fellesbetegnelsen «intelligente personlige assistenter», med forkortelsen IPA. Jeg vil benytte meg av assistentens navn (Alexa og Google Assistant) i tilfeller det er snakk om den ene eller den andre. Jeg benytter meg også vekselsvis av begrepet assistenten(e) hvis IPA blir nevnt mye i et avsnitt. Dette er gjort for lesbarhetens skyld.

1.4.2. Forbruker og informant

Per i dag defineres ikke begrepet «forbruker» i forbrukerkjøpsloven, men et grunnkrav er at kjøpet av en vare eller tjeneste er til privat bruk. Enten av kjøperen selv, eller til noen i hans eller hennes familie, eller omgangskrets (Lovdata, 2002). Ettersom denne studien kun vil fokusere på mennesker som bruker en IPA til privat bruk har jeg valgt å benytte meg av begrepet forbruker. I tillegg vil jeg benytte meg av begrepet informant i kapitlene hvor det er snakk om deltakerne i studien. Dette for å skille mellom hva tidligere forskning sier, og hva mine utvalgte informanter sier i sine intervjuer.

1.4.3. Artificial Intelligence

AI er forkortelsen av det engelske begrepet Artificial Intelligence. Den norske oversettelsen er kunstig intelligens. Forkortelsen AI er noe som jevnlig brukes i norske og engelske tekster, og for å holde språket konsekvent, vil jeg benytte meg av forkortelsen AI gjennom studien.

1.4.4. Internet of Things

IoT er en forkortelsen av det engelske begrepet Internet of Things. Den norske oversettelsen er tingenes internett. Forkortelsen IoT er et begrep som ofte brukes i norsk sammenheng, og det er et samlebegrep mange mennesker er kjent med. Derfor vil jeg benytte meg av den engelske forkortelsen IoT konsekvent gjennom studien.

1.5. Studiens design

Jeg vil nå kort presentere studiens oppbygging og hva som inngår i hvert kapittel.

Kapittel 1 presenterer oppgavens problemstilling og tema, samt hvordan jeg vil gå frem for å besvare problemstillingen gjennom analytiske dimensjoner.
Kapittel 2 er en gjennomgang av de teoretiske perspektivene som fungerer som undersøkelsesdimensjoner og rammeverk for analysekapitlene. I tillegg blir det redegjort for teknologien bak IPA, for å gi en grunnleggende forståelse for hva en slik assistent kan gjøre, hvordan den er bygget opp, og hvordan den er koblet sammen med andre enheter i forbrukeres hjem.
Kapittel 3 tar for seg metodiske valg, forskningsdesign, utvalg av informanter og rekrutteringsprosessen. I dette kapittelet blir det redegjort for valg som er gjort underveis i prosessen.
Kapittel 4 er analysens første kapittel. Her utforsker jeg informantenes holdninger til fenomenet overvåking.
Kapittel 5 er analysens andre kapittel. Her utforsker jeg informantenes holdninger til eget personvern og personvernets viktighet. I tillegg undersøker jeg hvordan kontekstuell integritet (forventinger til personvern) spiller inn for at de skal føle seg trygge i bruken av IPA.
Kapittel 6 er analysens tredje kapittel. Her utforsker jeg informantenes holdninger til påvirkning i form av målrettet annonsering, og hvorvidt de føler seg mottakelig for påvirkning.
Kapittel 7 er analysens siste kapittel. Her utforsker jeg informantenes holdninger til den feminine personligheten som er standard-setting for IPA. Hvilke valg ligger til grunn for valg av stemme, og hvordan påvirker dette forholdet mellom forbruker og IPA?
Kapittel 8 er studiens avsluttende kapittel hvor det blir gjort oppsummerende konklusjon av studiens funn i forhold til problemstillingen.

2. Teoretisk tilnærming

I mitt teorikapittel vil jeg presentere tidligere forskning, og relevante teoretiske perspektiver som belyser studiens problemstilling. For å finne relevant teori har jeg benyttet meg av bøker og forfattere jeg har fått kjennskap til gjennom studiet, forslag og tips fra veileder, akademiske søkemotorer som Google Scholar, Research Gate og SAGE, i tillegg til artikler fra IEE og Surveillance and Society, og universitetsbiblioteket Oria.

2.1. En digitalisert hverdag

Problemstillingen har som mål å kartlegge forbrukeres tanker og refleksjoner rundt overvåking og personvern i bruken av IPA. Så hva er egentlig en IPA, og hvilke konsepter og teknologier består de av?

Intelligente personlig assistenter er talestyrte høyttalere som bruker AI-teknologi til å gjenkjenne stemmer, skjønne hva som sagt eller spurt om, og respondere deretter (NRK, u.d.). AI-teknologien er det som gjør assistenten smart, og ifølge Bjørkeng (2019), kan AI beskrives som en type dataprogrammer som lærer fra miljøet rundt, og dermed kan denne type teknologi nå svært komplekse mål (Bjørkeng, 2019, s. 17). Det er antatt at populariteten rundt IPA vil øke kraftig de neste årene, ettersom teknologien er under kontinuerlig utvikling. I tillegg kan stadig flere IoT-enheter styres ved hjelp av assistenten (Ali & Yusuf, 2018). I dag finnes AI-teknologi i veldig av tingene rundt oss, som f.eks mobiltelefoner, dataspill, musikktjenester og GPS-tjenester. Når du strømmer innhold, scroller på Facebook eller leser nettaviser er det AI som tar beslutninger og foreslår hva du bruker tiden på (Bjørkeng, 2019, s. 9). AI-teknologi er i tillegg ønsket velkommen inn i mange hjem. I slike hjem kan for eksempel romtemperatur stille seg selv etter ulike behov, lys kan stilles etter tiden, og ikke minst bruken av intelligente personlig assistenter, som kanskje er det mest fremtredende beviset på at AI bli integrert inn i hverdagen (Agarwal, 2020).

Måten IPA kan kommunisere, og styre andre ting i hjemmet, er ved hjelp av konseptet IoT, som er betegnelsen på et nettverk hvor «ting» eller enheter med innebygde sensorer er sammenkoblet gjennom et privat eller offentlig nettverk (Khan & Salah, 2018, s. 395). Gjennom små sensorer og trådløs kommunikasjon kan et mangfold av ulike produkter kommunisere med hverandre, og med internett (Øverby, 2020). IoT-enheter kan være alt fra små personlig ting som klokker og telefoner, til større ting som kjøleskap, TV-er og IPA

(Atlam & Wills, 2019). IoT representerer en revolusjonerende måte å bruke internett på, ettersom enhetene kan kommunisere med hverandre, og dele data for å lage nye tjenester og applikasjoner, som igjen kan forbedre vår livskvalitet (Atlam & Wills, 2019, s. 123).

2.1.1. Avvik vekker bekymring

Det er tidligere gjort forskning på brukeratferd i forbindelse med IPA. Studier viser at IPA-brukere stort sett er komfortable i bruken av assistentene, så lenge det er i tråd med standard-konteksten de forventer. Det vil si, spørsmålet deres blir overført til Google eller Amazon, og de får svar kun basert på spørsmålet de stilte. Alle avvik fra denne standard-konteksten vekket umiddelbar bekymring hos respondentene. Eksempler på slike avvik kan være annonser og reklame i stedet for svar, eller svar fra en tredjepart (Malkin m.fl, 2019).

I en tverrkulturell undersøkelse med fokusgrupper i Nederland og USA kunne studien konkludere med at respondentene deres så mange fordeler med IPA-teknologien, men de hadde også tydelig bekymringer. Spesielt tre temaer gikk igjen som forbrukernes bekymringer. Det første temaet var en overdreven tro på, og avhengighet av teknologi, som blir en slags teknologisk kontroll. Det andre var sikkerhetsrisikoen ved at teknologien kjenner til personlig rutiner. Det tredje temaet var frykten rundt teknologiske sårbarheter, i form av hacking (Pridmore, et al., 2019).

2.2. Fenomenet overvåking

Fenomenet overvåking er ingenting nytt. Det er like gammelt som samfunnet selv. Mennesker har alltid overvåket hverandre, enten av sikkerhetsmessig årsaker, eller for å holde øye med hva andre driver med (Lyon, 2003). Likevel har overvåkingsmetoder og systematisk overvåking av enkeltindivider tatt mer spesifikke former i nyere historie, og nye teknologiske systemer har blitt implementert i prosessen (Lyon, 2006, s. 3).

Lyon (2007, ss. 14-15) definerer overvåking som systematisk, fokusrettet og rutinemessig informasjonsinnhenting av personlige detaljer med en hensikt om å påvirke, beskytte eller styre. Han beskriver det som fokusrettet fordi det retter oppmerksomheten mot enkeltpersoner, systematisk fordi informasjonen som samles inn ikke er tilfeldig, og rutinemessig fordi det oppfattes som en normal del av hverdagslivet.

2.2.1. Overvåkingstjenesten Alexa

For Amazon, med sin IPA «Alexa», er målet å tilby en sømløs og personlig service, og ikke minst tilegne en personlighet til merkevaren (West, 2019, s. 29). Hensikten med en alltid-lyttende mikrofon, er å starte datainnsamlingen så fort triggerordet er sagt, for så å lagre innsamlet data i nettskyen. Enheter med integrert kamera inneholder bevegelsessensorer. I dette tilfellet vil det å gå foran kamera være tilsvarende med å si triggerordet (West, 2019, s. 29). Til tross for at datainnsamlingen ikke skal skje før sensoren er utløst, eller triggerordet sagt, er det tidligere rapportert om tilfeller hvor dette ikke har blitt overholdt. I USA ble Alexa aktivert under en privat samtale mellom et ektepar. Samtalen ble så sendt videre til et vilkårlig telefonnummer i deres kontaktliste (Wolfson, 2018). I en artikkel fra Surveillance and Society blir det hevdet at Amazon ikke bare samler inn data som blir generert når forbrukeren benytter seg av tjenesten, men at de designer tjenester med den hensikt å samle inn enda mer forbrukerdata (West, 2019). Med en større internasjonal synlighet enn andre konkurrenter, og med en bredere integrering av IoT-enheter, er dette et forsøk på å gjøre Alexa til en uunnværlig tjeneste for forbrukerne; en tjeneste som åpner dørene for overvåking i flere private rom og situasjoner (West, 2019).

Amazon tilbyr å tjene oss ved å kjenne oss. Gjennom kjøp, produktsøk, medievaner, og interaksjoner med assistenten lærer de oss å kjenne gjennom *hva* vi sier, og *hvordan* vi sier det. Som West (2019) argumenterer, tilrettelegger Amazon for opplevelsen av å bli sett og tatt hensyn til. Samtidig utsetter vi oss for overvåking fra et enormt selskap, og dette blir normalisert gjennom den varme og kjente personligheten til assistenten (West, 2019).

2.2.2. De få vokter de mange

Overvåking er som nevnt tidligere ikke et nytt fenomen, og det skjer i ulike settinger hele tiden. Det kan være foreldre som tar i bruk enkelte overvåkingsmetoder for å beskytte barnet sitt, som for eksempel stedslokasjon på barnets mobiltelefon. Det kan være livvakter på stranden som følger med på badegjestene, eller en politipatrulje som holder øye med en mistenksom person eller gruppe som oppholder seg på en parkeringsplass (Lyon, 2007, ss. 14-15). En overvåkingsteori som har blitt koblet til den digitale tidsalder, er Michel Foucaults mye omdiskuterte panoptikon-konsept (Lyon, 2006, s. 4).

Foucaults teori er en videreføring av Jeremy Benthams fengselssystem fra 1799, hvor få fangevoktere kunne overvåke alle de innsatte ved å konstruere fengselet i en sirkel.

Fengselscellene hadde glasstak, og fangevokterne satt i et vakttårn i midten. Dermed kunne én fangevokter overvåke alle fangene (Mathiesen, 2013, s. 40). I den digitale alder er markedsføringsstrategien å treffe riktig mennesker med riktig annonse. Basert på innsamlet data kan selskaper skape en sosial profil og kategorisere konsumere i ulike grupper (Campbell & Carlson, 2002). Disse to tilsynelatende svært forskjellig fenomenene er likevel basert på en og samme teknikk; overvåking (Campbell & Carlson, 2002).

Benthams fengselssystem er altså basert på en lukket sirkel som med få ressurser ga full kontroll over de innsatte. I den digitale tidsalder er overvåking ifølge Campbell og Carlson (2002) en nøkkelmekanisme for kapitalister til å sikre seg sosial kontroll, og dermed forutsigbarhet av forbrukerne på markedet (Campbell & Carlson, 2002). Ifølge Zuboff var denne lukkede sirkelen som Bentham konstruerte i panoptikon-fengselet ment til å skape betingelsen om at det ikke fantes noen utgang (Zuboff, 2019, s. 491). Når det gjelder nåtidens overvåking, mener hun vi befinner oss i en liknende situasjon. Hun mener det ikke finnes noen utgang fra overvåkingen. Men det er ikke lenger fengselsvoktere som følger med på fangende. Det er overvåkingskapitalister som følger med på alle. Og igjen er det de få som vokter de mange. (Zuboff, 2019, s. 471)

2.3. Overvåkingskapitalisme

Har du noen gang fått reklame som tilsynelatende er basert på produkter du føler du nettopp har snakket om, eller søkt etter på internett? Hvorfor annonsene du blir eksponert for ofte dekker behovet ditt akkurat nå? Shoshana Zuboff skapte et begrep for dette nye fenomenet, nemlig *overvåkingskapitalisme*. Zuboff definerer overvåkingskapitalisme som en ny økonomisk orden som bruker menneskelig erfaringer som en slags råvare brukt for kommersiell utvinning, forutsigbarhet og salg (Zuboff, 2019). Moderne, digitale plattformer, som netthandel, kommunikasjon og smarte infrastruktursystemer, produserer enorme mengder detaljerte data om brukeren. Alt fra deres preferanser og mønster i adferd, til deres håp, tro og ønsker (Cinnamon, 2017). Selskapene som kontrollerer disse dataene sitter med en enorm økonomisk verdi, fordi dataene blir produsert av forbrukere uten noen form for økonomisk kompensasjon. I tillegg er det et raskt voksende marked for andre selskaper som ønsker å kjøpe disse dataene (Cinnamon, 2017).

Dette råmaterialet av menneskelig erfaringer, blir ifølge Zuboff (2019) analysert til forutsigbar oppførsel, som igjen kan bli brukt i «machine intelligence». Dermed er det mulig å forutse hva dine neste trekk sannsynligvis vil være: hva du vil gjøre nå, snart, og i fremtiden. Denne forutsigbarheten er noe mange selskaper ønsker å involvere seg i (Zuboff, 2019, s. 8). Overvåkingskapitalismen har vokst seg frem på grunn av utnyttende avtaler mellom individ og datainnsamlere. Avtalen blir kritisert for å være utnyttende fordi de fleste har utilstrekkelig kunnskap rundt omfanget av datainnsamlingen (Cinnamon, 2017). Peacock (2014, s. 8) beskriver denne utnyttende avtalen som samvittighetsløs, urettferdig og uunngåelig, og noe brukere ikke har anledning til å forhandle om. Deres eneste alternativ er å være offline.

2.3.1. Google baner vei for overvåkingskapitalismen

Da Google ble etablert i 1998, var deres ønske at informasjon skulle være en befriende og demokratisk sosial styrke. De fant fort ut at informasjonen som fulgte med brukeres søk på Google, kunne blir gjenvunnet i en prosess av kontinuerlig maskin-læring (Zuboff, 2019, s. 68). Til tross for at andre søkemotorer på 1990-tallet hadde samme mulighet som Google til å ta i bruk informasjonen brukere la igjen etter å ha brukt tjenesten, var det ingen som så verdien i å samle opp denne informasjonen og ta den i bruk. Men det gjorde Google. Derfor kan Google sies å være en pioner, utvikler, eksperimentator, ledende utøver og rollemodell innenfor overvåkingskapitalismen, ifølge Zuboff (2019, s. 63). Googles utnyttelse av disse overskuddsdataene var med andre ord starten for overvåkingskapitalismen, og de har over tid perfeksjonert denne type kapitalisme. I dag lages produkter med den hensikt å suge til seg hver eneste bit med informasjon på det digitale kartet (Thornhill, 2019). Alt fra IPA til termometere. Fra nettshopping og handlevaner, til selvdrevne bilder og smart-hjem. Alt har blitt et mål for å samle inn data. Overvåkingskapitalistene kan spionerer på sine brukere, uten at brukeren vet hva som foregår. (Thornhill, 2019)

2.3.2. Manipulasjon og politisk påvirkning

Flere teoretikere har som nevnt tidligere dratt paralleller mellom Jeremy Benthams fengselssystem, panoptikon, fra slutten av 1700-tallet, og overvåkingen som skjer i den digitale alder. Zuboff sammenlikner panoptikon med dagens situasjon fordi hun mener at vi også nå befinner oss i en lukket sirkel, hvor det ikke er mulig å slippe unna overvåkingen. Med et stadig voksende IoT-marked, og flere hjem som blir smarte, får vi sensorer rundt oss på alle kanter. Alt fra kjøleskapet og komfyren på kjøkkenet, til klokken du har på deg, IPA-

en i stua, GPS-en i bilen og tannbørsten på badet kan i dag inneholde sensorer, som alle har evnen til å lagre dine data. Zuboff argumenterer for at sensorene i IoT-enheter ikke lenger bare blir brukt som allestedsnærværende datasamlere og -behandlere, men at det nye målet har blitt inngrep, handling og kontroll (Zuboff, 2019, s. 292). Det betyr at de registrerer og analyserer oppførselen til forbrukeren, og finner ut hvordan de kan *endre* denne oppførselen (Zuboff, 2019, s. 292).

Det høres kanskje søkt ut at selskaper kan klare å endre din oppførsel basert på små biter med informasjon, som du kanskje ikke engang tenker er informasjon. For eksempel hvor lang tid du bruker på en nettside, hvilke e-poster du åpner, hvilke produkter du har kikket på, og hvilke omtaler du har lest, høres svært lite verdifullt ut hver for seg. Men alt dette føyer til en liten bit med detaljer til det komplekse puslespillet som er deg. Små detaljer om deg kan gjøre det enklere å vite hvilke inntrykk du skal utsettes for, for størst mulig påvirkning (West, 2019).

Et slikt tilfelle av påvirkning har blitt mye omdiskutert etter USAs presidentvalg i 2016, hvor selskapet Cambridge Analytica jobbet med Donald Trumps presidentkampanje. Det har blitt diskutert hvorvidt de klarte å påvirke valget i Trumps favør (Press, 2018). En «personlighetstest», som krevde Facebook-tilgang, ga ikke bare tilgang til informasjon om personer som tok testen, den ga også informasjon om alle deres Facebook-kontakter. På den måten samlet selskapet inn informasjon fra 87 millioner Facebook-profiler uten deres samtykke. Alexander Nix, Cambridge Analyticas tidligere sjef, hevdet at de hadde kartlagt personlighetsegenskapene til alle voksne personer i USA (Press, 2018). Deretter fikk personer målrettet reklame som spilte særlig på frykt og følelser, basert på deres personlighetstype. (Press, 2018). For eksempel, velgere med stor fremmedfrykt ble eksponert for valgannonser som spilte på homofilt ekteskap, arbeidsledige kunne bli eksponert for valgtemaer som omhandler tapet av amerikanske jobber og så videre (Berghel, 2018). Dr. Hal Berghel ved Universitetet i Nevada, mener målrettet annonsering på sosiale medier lar politiske kampanjer spille på våre sterkeste følelser og frykt, og kan manipulere lettpåvirkelige mennesker (Berghel, 2018).

2.3.3. Den trojanske hesten

I en film fra 2017 med tittel «The Circle», spiller Tom Hanks grunnleggeren i et tek-selskap som ønsker totalt åpenhet og demokrati i samfunnet ved å lage sosiale profiler basert på

informasjon innhentet fra klokker, kameraer, mikrofoner, private e-poster og sosiale medier. Overvåkingen sørger for at det ikke er mulig å holde noe skjult på godt og vondt, og nå, fire år etter at denne thrilleren ble lansert, er det flere likheter mellom virkelige selskaper som Google, Apple, Amazon og oppdiktede The Circle. Denne fiksjonsfilmen kan nemlig i stor grad minne om Zuboffs beskrivelse av den digitale fremtid. Zuboff definerer og beskriver et begrep for fremtiden innen teknologi, nemlig «inevitibalism». På norsk kan dette oversettes til «uungåelighet». Ifølge Zuboff er lederne i Google, sammen med flere andre eksperter i den teknologidrevne regionen i California, Silicon Valley, nærmest bestemt på at allestedsnærværende datainnsamling vil spre seg til alle aspekter av livene våre. Det er en tro på at en fremtid hvor nærmest alt og alle er sammenkoblet i et IoT-nettverk er uungåelig (Zuboff, 2019, ss. 222-223). Ifølge Zuboff har de såpass stor tro på nettopp dette, at hun definerer «inevitabilism» som en ideologi (Zuboff, 2019, s. 221). Et særlig viktig poeng Zuboff påpeker, er hvordan «inevitabilism» utelukker valg og frivillig deltakelse. Det vil dermed ikke gi rom for menneskelig vilje i fremtiden (Zuboff, 2019, s. 226). Denne nye ideologien av datamediert kommunikasjon kommer inn i livene våre som en trojansk hest. Med sine apper, enheter og tilkoblinger, blir vi distrahert med suksessen fra den høyst bevisste overvåkingskapitalismen, men ifølge Zuboff risikerer vi å sitte igjen med en følelse hjelpeløshet (Zuboff, 2019, s. 342).

2.3.4. Identifikasjonspuslespillet

Kanskje tenker du at små biter med informasjon om deg umulig kan ha noe særlig verdi for andre. Det spiller kanskje ingen rolle om du legger igjen navnet ditt på en nettside, eller at Google kjenner til adressen din, hvilket politiske parti du stemmer, eller hvor religiøs du er? Ifølge Gandy (2011) er det vanskelig å fastslå verdien av slik personlig informasjon. Brukere vet sjelden hvilke type informasjon de selv ser på som verdifull (Gandy, 2011, s. 446). Han mener likevel at finnes informasjonskategorier med ulike prisnivåer, basert på brukerens antatte verdi av informasjonen. Hver enkelt bit informasjon er ikke nødvendigvis viktig eller særlig verdifull alene, men verdien skapes når hver ekstra bit med informasjon skaper en profil av en forbruker som tilsammen muliggjør identifisering og klassifisering av individet. Nøkkelen for selskaper er å få tak i den biten med informasjon som løser identifikasjons-puslespillet, som kan resultere i et lite konkurransefortrinn for selskapet (Gandy, 2011, s. 446).

På denne måten kan små informasjonsbiter om deg være med å putte din brukerprofil inn i en bestemt kategori. Dermed kan informasjon om hvem du stemte på ved forrige valg, om du donerer til veldedig organisasjoner, eller om inntekten din er over en viss grense være verdifull, dersom du faller inn under kategorien med mennesker noen ønsker å kontakte (Gandy, 2011, s. 446). Markedsførere ser seg gjerne ut en spesiell målgruppe de ønsker å målrettet nå ut til. Her bruker Gandy (2011) butikkers lojalitetsprogram som et eksempel, hvor god kundeoppførsel blir belønnet, og at dette er med på å forme et langvarig og stabilt forhold mellom forbruker og distributør (Gandy, 2011, s. 446).

Overvåkingskapitalismen blir altså beskrevet som en ny form for kapitalisme, hvor menneskelig erfaringer blir brukt som råmateriale til å analysere og forutse forbrukernes fremtidige trekk. Informasjonen blir samlet inn gjennom ulike enheter og apparater, og det er det totale bildet av forutsigbarhet som kan være svært verdifullt for selskaper. Hva du vil gjøre nå, snart og i fremtiden (Zuboff, 2019). Avtaler mellom de som samler inn dataen og individer blir kritisert for at være samvittighetsløs og urettferdig, fordi det ikke er mulig å forhandle om egne data. Forbrukeres eneste alternativ i praksis blir å være offline. Med Google i spissen blir overvåkingskapitalister anklaget for å spionere på sine brukere uten at de vet hva som foregår (Thornhill, 2019). På en annen side kan det kanskje ikke kalles spionasje når brukeren selv har godkjent personvernserklæringen. Dermed får personvernet altså en sentral rolle i overvåkingskapitalismen, og det kan være vanskelig som forbruker å forstå hvilken verdi personvernet har.

2.4. Personvernets verdi

Mange ville nok sagt seg enig i at personvern er viktig for å verne om personlige opplysninger. Men hvilken verdi har personvernet egentlig? Hvem er det man beskytter opplysningene fra? I 1997 beskrev James H. Moor datidens utfordring som det å finne en måte å utnytte mulighetene datamaskiner gir oss, uten å selv bli utnyttet av datamaskiner og datalagring. Han mente personvern er noe som bør sees på som todelt. På den ene siden kan det virke som noe veldig bra, og noe vi alltid bør strekke oss langt for å beskytte. På den andre siden kan det se ut til at personvern lettere defineres av personlig preferanser, kulturelle påvirkninger og noe det er generelt vanskelig å fastslå viktigheten av (Moor, 1997). Han diskuterer tre måter å definere personvern, og hvilken verdi personvern har. Jeg vil nå se nærmere på hans tre definisjoner.

2.4.1. Personvernets instrumentelle verdi

Instrumentell verdi kan defineres som noe som har en verdi, fordi det er et middel eller en mulighet til å realisere eller oppnå noe med egenverdi, som ofte er et mål i seg selv (Sagdal, 2019). Moor (1997) argumenterer for at de aller fleste vil være enige om at personvern har instrumentell verdi. Det beskytter oss og informasjonen vi ønsker eller trenger å holde for oss selv. Dette kan for eksempel vises i en persons sykehistorikk. Tabubelagte diagnoser kunne for eksempel ført til diskriminasjon i jobbansettelse eller forsikringssaker, dersom personens sykehistorikk hadde vært offentlig og tilgjengelig for alle (Moor, 1997, s. 29). Andre eksempler kan være seksuell legning som kunne ført til diskriminering, eller kanskje hobbyer og interesser man ønsker å holde for seg selv. Det er ikke all informasjon vi ønsker å dele med resten av verden. Personvernet blir derfor viktig som et middel til å beskytte noe som har egenverdi for oss.

Marwick og Boyd (2014) er blant dem som diskuterer personvern på nett, og argumenterer for at unge mennesker ofte benytter seg av en rekke taktikker i et forsøk på å få kontroll over hvilken informasjon som blir delt, og hvem som får tilgang til informasjonen (Marwick & Boyd, 2014, s. 6). En slik taktikk kan være å monitorere personverninnstillingene, slik at kun menneskene som er ment å se innholdet, får sett det. På denne måten kan man dele interne spøker og informasjon med vennene sine, uten at snokete foreldre eller søsken får det meg seg (Marwick & Boyd, 2014).

2.4.2. Personvernets egenverdi

Moor argumenterer for at personvern ville vært mer sikret, hvis man kunne bevise at det har egenverdi. Han trekker frem Debora Johnsons (1994) påstand om at personvern er en essensiell del av menneskers selvstyrerett. Så hvis selvstyrerett har egenverdi, og personvern er en vesentlig del av selvstyreretten, slik Johnson (1994) mener, så kan man argumentere for at personvern også har indirekte egenverdi (Moor, 1997, s. 28). Likevel utfordrer Moor denne tanken ved å trekke frem et interessant eksempel. Si man blir konstant overvåket av «Tom», som er svært begavet når det gjelder datamaskinbruk, og han bruker denne kunnskapen til å få vite alt om deg. Han har installert kameraer og følger med på alle dine bevegelser, uten at du selv er klar over det (Moor, 1997, s. 29). Som Moor argumenterer, ville de fleste tenkt at slik overvåking ville vært ubehagelig, selv om informasjonen ikke ble delt videre eller brukt til å

skade deg. Dermed ville du hatt full selvstyrerett, men ikke lenger noe privatliv eller personvern mot «Tom» sin overvåking (Moor, 1997, s. 29). Han utfordrer med dette Johnsons (1994) påstand om at personvern er essensielt for menneskers selvstyrerett.

2.4.3. Personvernets kjerneverdi

Moors tredje måte å definere personvern på, er hans egen tolkning i et forsøk på å beskrive personvernets viktighet. Han beskriver kjerneverdiene, som han argumenterer finnes i ethvert samfunn i varierende grad som liv, lykke, frihet, kunnskap, evner, ressurser og sikkerhet (Moor, 1997, s. 30). Han beskriver kjerneverdiene som rammeverket, men innenfor rammeverket er det rom for individuell og kulturell variasjon (Moor, 1997, s. 30). Når samfunn blir større, mer interaktive og mindre intime, blir personvern en form for sikkerhet, som ifølge Moor (1997, s. 30) er en kjerneverdi.

Moor konkluderer med at ved å bruke kjerneverdiene som et rammeverk, så kan personvern defineres som å ha både instrumentell verdi, da det er en støtte for alle kjerneverdiene, men også som å ha egenverdi, da det er en måte å uttrykke sikkerhet (Moor, 1997, s. 30). Moors forsøk på å definere personvern kan altså til kokes ned til å handle om sikkerhet. Likevel kan det argumenteres for at et så komplekst fenomen som personvern ikke alltid er like svart-hvitt. Det er ikke nødvendigvis slik at et brudd på personvernet alltid fører meg seg en sikkerhetsrisiko. I de fleste tilfeller er det konteksten rundt informasjonsdelingen som er avgjørende for hvorfor et personvernbrudd oppstår, og dette er noe Helen Nissenbaum (2010) diskuterer.

2.5. Kontekstuell integritet

Har du noen gang følt at personvernet ditt har blitt brutt eller krenket? Sannsynligheten er nok stor for at du kan svare ja på det. Kanskje har noen delt informasjon om deg som de ikke skulle dele videre, eller et selskap har videresendt din mailadresse, og nå får du masse reklame du ikke har sagt ja til. Det er mange måter å føle at personvernet ikke har blitt ivaretatt på, og det er ingen konkret måte å definere hvor grensen går. For min del følte jeg det var et brudd på personvernet mitt da jeg fant ut at alt jeg sier til min IPA blir lagret, og kan bli lyttet til av ansatte i Google. Det er ikke det at ting jeg sa til assistenten var hemmelig i den forstand, det hadde ingenting med informasjonskarakteren å gjøre. Det var heller det at jeg

følte interaksjonene mellom meg og assisten ikke var ment for andres ører, og de var ikke ment å bli lagret permanent.

I noen tilfeller er personvernbrudd svart-hvitt. Om din fastlege hadde delt informasjon om din sykehistorie med noen som ikke er relevant helsepersonell, ville dette selvsagt vært et tydelig brudd på både personvern og taushetsplikt. Om en venn deler informasjon om deg, ville du kanskje følt det var greit om det var til en annen god venn, men opplevd det som et tillitsbrudd om det var til en du hadde konflikt med. Det hele handler om konteksten. Helen Nissenbaum (2010) har derfor utviklet et rammeverk som hun kaller kontekstuell integritet. Konseptet evaluerer flyten av informasjon om enkeltpersoner utfra gitte kontekstuelle normer. Slike normer kan bli definert av informasjonens emne, hvem som er avsender og mottaker, type informasjon og hvordan informasjonen er overført. (Nissenbaum, 2010). Den kontekstuelle integriteten blir krenket når en eller flere av normene knyttet til et spesielt forhold brytes (Taft, 2019, s. 3). Rammeverket vil kunne redegjøre for faktorer som avgjør når folk oppfatter ny informasjonsteknologi og nye systemer som en trussel mot personvernet. Ikke bare vil det kunne forutsi folks oppfatning, men også presentere en tilnærming til å evaluere disse systemene, og hvordan man kan håndtere personvernsaker (Nissenbaum, 2010, s. 1).

Bakgrunnen for denne personvernmodellen, argumenterer Nissenbaum, er at tidligere teorier rundt personvern gir viktig informasjon og innsikt, men de er for generelle. Hun argumenterer for at tidligere modeller skiller gjerne mellom offentlig og privat, og dermed ikke gir nok innsikt i forskjellig variabler som kan forekomme i kontekstuell integritet (Nissenbaum, 2004). Spesielt gjelder dette innenfor nye teknologi-baserte systemer, som gir store hull i tidligere anvendte prinsipper for personvern (Nissenbaum, 2010, s. 232). Informasjonsteknologi er regnet å være en enorm trussel for personvernet, fordi det gir rom for overvåking, store databaser, og deling av informasjon rundt hele verden i lysets hastighet (Nissenbaum, 2010, s. 1). Før jeg presenterer nøkkelprinsippene i kontekstuell integritet, er det viktig å ha en forståelse for hvilke situasjoner teorien har sitt opphav fra. Kontekstuell integritet har som hensikt å fungere som et rammeverk innenfor sosioteknologiske systemer, altså enheter som lar oss kommunisere med hverandre.

2.5.1. Sosioteknologiske systemer

Nissenbaums teoretiske modell baseres på ideen om at retten til personvern ikke betyr retten til hemmelighold, kontroll, begrense eller hindre andres tilgang til din informasjon. Kontekstuell integritet handler om retten til å leve i en verden hvor våre forventninger rundt personvern stort sett blir møtt, og at disse forventingene er basert på, og i samsvar med, nøkkelprinsipper i det sosiale livet. Kontekstuell integritet er ifølge Nissenbaum oppnåelig gjennom å finne balansen mellom sosiale normer og regler, med både lokale og generelle verdier, mål og formål. (Nissenbaum, 2010, s. 231) Teorien til Nissenbaum kan derfor bli brukt til et rammeverk i situasjoner hvor nye teknologiske systemer kan bli oppfattet som en trussel mot personvernet, og hvordan man kan løse dette (Nissenbaum, 2010, s. 3).

Sosioteknologiske systemer er hva Nissenbaum beskriver som teknologi som lar oss kommunisere med hverandre. Enheter som telefoner, internett og datamaskiner. I tillegg er det enheter som er knyttet sammen, og som sender og mottar personlig informasjon (Nissenbaum, 2010, ss. 4-6). Da Nissenbaums teori ble skrevet i 2010 var ikke for eksempel smart-assistenter kommet på markedet, og mye har skjedd på ti år hva gjelder egenskapene til smart-telefonen, og ikke minst hvor mye vi kommuniserer gjennom slike sosioteknologiske systemer. Jeg har valgt å benytte meg av Nissenbaums teoretiske perspektiv da jeg mener dagens utfordringer rundt personvern og sosioteknologiske systemer er like aktuelle i dag, om ikke mer, enn hva det var for 11 år siden.

Sosioteknologiske enheter og systemer kontrollerer, håndterer og styrer strømmen av personlig informasjon. Det er gjerne disse som har vært knyttet til mistanke, angst og har ofte vært bakgrunnen for det som ofte har blitt oppfattet som en trussel eller brudd på personvernet (Nissenbaum, 2010, s. 6). Likevel er det viktig å skille mellom forskjellig typer sosioteknologiske systemer, for ikke alle systemene har gitt grunn til bekymring. Innen helsesektoren kan slike enheter og systemer brukes til å hjelpe helsevesenet i en travel hverdag, og kan være en ressurs ved å måle blodtrykk, puls, og kan holde øye med pasientens helse (Nissenbaum, 2010, s. 6). Kanskje kan slike systemer la eldre bo hjemme lenger, og det kan være en ressurs for helsevesenet ved å kunne fjern-monitorere pasienter. Kontrasten er de sosioteknologiske systemene som for eksempel overvåker parker, enkeltpersoners handlevaner, telefonavlytting eller overvåking av netthandel. Begge eksemplene beskriver en informasjonsflyt, men én er ønsket velkommen, og én blir møtt med skepsis og motvilje (Nissenbaum, 2010, s. 6). Den teoretiske modellen jobber derfor mot å finne ut hvor skillet

går, og hva det er som skaper uenighet og konflikt hva gjelder personvern. Dermed foreslår hun et rammeverk for å løse eller minimere konflikten.

2.5.2. Nøkkelprinsipper i kontekstuell integritet

Rammeverket som er utviklet for å minimere konflikten beskrevet overfor baseres på fire nøkkelprinsipper: normer, aktører, informasjonskarakter og overvåkingsprinsipper.

Normer er menneskers forventing til oppførsel, og forventing til hvordan informasjon skal bli håndtert. Dette er viktig for å avgjøre den kontekstuelle integriteten. Det kan skilles mellom to hovedtyper av *informasjonsnormer*, hvor den ene er *deskriptive normer,* som er normer man ikke nødvendigvis må følge, men som de aller fleste følger. Dette blir ansett som normal oppførsel. Den andre typen er *injunktive normer,* som er normer folk mener burde følges, og dette anses som sosialt akseptabel/uakseptabel oppførsel (Nissenbaum, 2010, s. 148). Nissenbaum vektlegger injunktive normer som dominerende, da folk flest følger normer da de mener dette er riktig, og sosialt akseptabel oppførsel (Nissenbaum, 2010, s. 148).

Informasjonsnormer har tre forskjellige *aktører*, eller deltakere. Disse kategoriseres som sender av informasjon, mottaker av informasjon, og informasjonsobjektet, som er den informasjonen handler om (Nissenbaum, 2010, s. 142). Aktørene i kontekstuell integritet er spesielt viktig, da det er aktørkonflikter som kan være grunn for at mennesker føler det har vært brudd på personvernet. Nissenbaum mener at det i situasjoner hvor folk føler det har vært brudd på personvernet, ikke nødvendigvis at innholdet i informasjonen som ble delt som er grunn til konflikt. Det er dermed ikke alltid at informasjonen var hemmelig, men problemet ligger ofte i det av man føler informasjonen ble delt på feil måte, med feil mennesker (Nissenbaum, 2010, s. 142).

En annen svært viktig faktor i kontekstuell integritet er *informasjonskarakter*. Hva informasjonen handler om. Informasjonsnormene er det som avgjør om informasjonen er passende eller upassende i gitte situasjoner, under visse forhold. Vi deler forskjellig informasjon med foreldrene våre, som vi deler med vennene våre. Vi deler forskjellig informasjon med legen vår som vi gjør med læreren vår, sjefen vår eller kollegaer på jobb. Variablene som avgjør hva som er passelig informasjon å dele varierer, på samme måte som at kontekst, normer og roller kan variere. Det er derfor vanskelig å presentere et klart skille mellom passende og upassende informasjonskarakter. (Nissenbaum, 2010, ss. 152-153)

Overføringsprinsipper setter en begrensing på informasjonsdeling fra en part til en annen. I noen tilfeller er det informasjonens natur som ligger til grunn for dette prinsippet, i andre tilfeller kan det være rollebestemmelser eller andre variabler. Et eksempel på et slikt prinsipp kan være at en part som har mottatt informasjon, ikke får lov til å dele det videre (Nissenbaum, 2010, s. 154). Dette illustreres godt i et venneforhold, hvor man er forventet å dele informasjon med hverandre frivillig. I dette tilfellet er det forventet at informasjonen som deles, avhengig av dens natur, ikke deles videre. Ofte vil det være akseptabelt å bevege seg litt utenfor grensen, som å dele noe som ikke blir sett på som hemmelig eller sensitivt, med en tredjepart. Går man derimot for langt ved å dele for mye informasjon med feil personer, eller få tak i informasjon på tvilsomme måter som å lese noens dagbok eller meldinger, vil det fort kunne ansees som et brudd på den kontekstuelle integriteten, og kan bli ansett som et svik mellom venner. (Nissenbaum, 2010, s. 154)

I noen situasjoner kan det være at noen har krav på informasjon. For eksempel en lege som trenger informasjon rundt en pasients helse som for å stille riktig diagnose. En hjelpepleier må videreformidle informasjon angående pasienten om smittsomme sykdommer til offentlig helsepersonell, eller kanskje må politiet vite informasjon rundt en straffbar handling. Det finnes altså flere mulige overføringsprinsipper i forskjellig situasjoner, basert på roller, normer og kontekst (Nissenbaum, 2010, s. 155).

Nissenbaums nøkkelprinsipper fungerer altså som et rammeverk for situasjoner som kan oppstå rundt sosioteknologiske systemer, og foreslår at det er konteksten rundt de forskjellige nøkkelprinsippene som vil være avgjørende faktorer når folk opplever brudd på personvernet. Informasjonsteknologi er regnet for å være en trussel mot personvernet fordi det gir rom for eksempelvis overvåking (Nissenbaum, 2010). I forbindelse med IPA hevder tidligere studier at overvåkingen potensielt sett skjer på et mer personlig plan, fordi enhetene er nøye utformet med menneskelige egenskaper, nettopp for å viske ut skepsisen mange ville hatt rundt det å ha en påkoblet mikrofon i hjemmet (West, 2019).

2.6. Antropomorfisme

Antropomorfisme betyr å tilegne menneskelig egenskaper som motivasjoner, intensjoner og følelser til et ikke-menneskelig objekt (Epley, Waytz, & Cacioppo, 2007). Begrepet

antropomorfisme brukes ofte om hverandre med begrepet personifisering (Pradhan, Findlater, & Lazar, 2019). I en studie gjort ved Universitetet i Maryland, og Universitetet i Washington, USA, ble det forsket på eldre voksnes forhold til stemmeaktivert smart-enheter, og hvorvidt begrepet antropomorfisme kan implementeres til disse ikke-menneskelige enhetene. Etter å plassert en Amazon Echo i hjemmene til syv mennesker fra 65-83 år i tre uker, samlet de kvalitative data gjennom intervjuer, dagbokføringer, og brukerlogg. Denne studien kunne konkludere med at i stedet for å kategorisere den stemmeaktiverte assistenten som enten «menneskelig» eller «objekt», flyter deltakernes oppfatning mellom begge kategoriene, men at brukere ser ut til å plassere den stemmeaktiverte assistenten i en av kategoriene over tid, og med vedvarende bruk. (Pradhan, Findlater, & Lazar, 2019)

Studien konkluderer altså med at forbrukere har en tendens til å veksle mellom oppfatningen om at assistenten er menneskelig eller et objekt, men at man gjerne plasserer assistenten i en av kategoriene etter vedvarende bruk. Denne studien har dog eldre respondenter, og kan dermed ikke nødvendigvis si noe om hvilken kategori yngre forbrukere plasserer enheten i.

2.6.1. Stereotypiske kjønnsroller

Stereotyper er ikke bare merkelapper, men det er antakelser om egenskaper og atferd folk i merkede kategorier antas å ha (Kite, Deaux, & Haines, 2008, s. 205). Fra tidligere studier er det konkludert med at generelt blir kvinner sett på som mer emosjonelle, mildere, mer forståelsesfulle og hengivne, mens menn blir ansett som konkurransedyktige, uavhengige og selvsikre (Kite, Deaux, & Haines, 2008, s. 207). I tillegg har forskere utvidet vår forståelse av kjønnsbaserte stereotyper ved å identifisere flere dimensjoner hvor vi gjerne skiller oppfatningen av kvinner og menn, som samfunnsroller. Menn blir sett på som ledere, økonomiske forsørgere og overhode i en husholdning, mens kvinner blir sett på som omsorgspersoner som handler, steller i hjemmet og opptrer støttende. (Kite, Deaux, & Haines, 2008, s. 207)

I en studie gjort ved Universitetet i Indiana ble det konkludert med at stereotypiske kjønnsroller er såpass integrert i menneskelig psykologi, at det overføres til teknologien (Moon & Green, 2006). Valg av stemme kan derfor påvirke forbrukeren, fordi man assosierer enheten med kjønnet stemmen er basert på. Hvor en mannlig stemme vil gi forventinger om respons basert på stereotypiske menn, vil en kvinnelig stemme vil gi forventninger om respons basert på stereotypiske kvinner (Moon & Green, 2006).

2.6.2. En kvinnelig omsorgsperson

Populære IPAer som Amazons Alexa, Apples Siri, Microsofts Cortana og Googles Assistant er standardinnstilt til å ha en kvinnelig stemme. I tillegg har tre av assistene kvinnelig navn (Schwär & Moynihan, 2020). Ifølge Schwär og Moynihan (2020) er bakgrunnen for den feminine fremtoningen til assistentene nøye kalkulert av utviklerne, og basert på forskning som viser at vi gjerne velger kvinner til å hjelpe- og assistere oss. I tillegg blir kvinnelig stemmer ofte blir sett på som mer tilfredsstillende og behagelige (Schwär & Moynihan, 2020).

En studie fra 2018 undersøkte hvordan den feminine fremtoningen i de virtuelle assistentene som Siri og Alexa er med på å skape en trygghet i hjemmet, for å få folk til å hyppigere samhandle med sin IPA. Studien kunne konkludere med at den feminine fremtoningen i en slik virtuell assistent begrunnes i stereotypiske kjønnsroller, hvor kvinnen blir sett på som en omsorgsperson, eksempelvis en mor eller kone. Siri og Alexa er begge utformet for å skape et forhold mellom enheten og forbrukeren, slik at skepsisen til selskapene bak viskes ut, og man inviterer overvåkingen inn på et mer intimt plan. (Woods, 2018)

De stereotypiske kjønnsrollene i IPA skaper en grobunn for kapitalismen til å ekspandere ved å menneskeliggjøre og seksualisere overvåkingsenheten, da deres persona er bygget for å fjerne angst og skepsis mange brukere kanskje ville hatt rundt det å ha en enhet i hus som kan kommunisere og styre smart-hjemmet deres (Woods, 2018).

Hvordan vi oppfatter vår IPA vil påvirke den økonomiske gevinsten for leverandøren. Det er nemlig ikke salget av selve enheten de tjener de store summene på. De tjener penger etter hvor mye brukerne samhandler med sin IPA. På denne måten vil stemmen til Alexa etterlikne en kvinne vi sosialiserer med, shopper med og spør om hjelp, fremfor en teknologisk enhet. Det er med andre ord shoppingen gjennom IPAen og datainnsamlingen som er den økonomiske gevinsten for de store selskapene (Schwär & Moynihan, 2020).

Antropomorfisme betyr altså å tilegne menneskelig egenskaper til noe som ikke er menneskelig. For eksempel kan man si at «solen smiler» eller at «himmelen gråter». Dette er relevant i bruken av IPA, ettersom den ikke bare kan snakke og samhandle med et menneske, men i mange tilfeller har assistenten fått et kvinnelig navn og stemme basert på stereotypiske kjønnsroller (Schwär & Moynihan, 2020). Hvilken stemme assistenten har, påvirker

forbrukeren, fordi man assosierer enheten med kjønnet stemmen er basert på (Moon & Green, 2006). Når assistenten har en kvinnelig fremtoning, vil dette assosieres med en kvinne vi sosialiserer med, og spør om hjelp, som for eksempel en mor, søster, venninne eller kjæreste (Schwär & Moynihan, 2020).

2.7. Oppsummering

Dette kapittelet presenterer tidligere forskning og teoretiske perspektiver som tilrettelegger for å gjennomføre analysen knyttet til de fire analytiske dimensjonene. Teorikapittelet belyser temaene overvåking, personvern, påvirkning og antropomorfisme. Før jeg analyserer studiens empiriske funn, vil jeg redegjøre for de metodiske valgene som er tatt gjennom studiens forløp.

3. Metode

Etter å ha lagt det teoretiske og analytiske grunnlaget for den empiriske analysen, vil jeg i dette kapittelet redegjøre for de metodiske valgene som er tatt gjennom studien. Prosjektet er registrert og godkjent i RETTE etter avtale med veileder (Vedlegg C). Prosjektets metodiske valg innebærer metodetilnærming, informantutvalg, utforming av intervjuguide, gjennomføring av intervjuer, samt utfordringer som har oppstått underveis, og hvordan jeg har valgt å løse dette. Aller først vil jeg kort redegjøre for studiens forskningsdesign.

3.1. Forskningsdesign

For dette prosjektet har jeg benyttet meg av kvalitativ metode, med et hermeneutisk tilnærming. Det vil si at jeg fortolker og søker etter en mening i datamaterialet. En slik tilnærming består av faser der man forstår deler i lys av helheten (Østbye et.al, 2013, s. 21). Fire analytiske dimensjoner er derfor benyttet for å forstå deler av informantenes helhetlige bevissthet rundt personvern og overvåking i bruken av IPA.

Ifølge Østbye et.al (2013) er det prosjektets perspektiver og problemstillinger som er avgjørende for hvilken metode som er mest passende (s. 103). Målet med et kvalitativt intervju er å bli kjent med informantenes holdninger og refleksjoner rundt personvern, overvåking og IPA. En kvalitativ metodetilnærming med semistrukturerte intervjuer åpner for muligheten til å observere informantenes kroppsspråk, få tilgang til deres begrepsapparat og ikke minst få informasjon det ellers ville vært vanskelig å fa tilgang til (Østbye et.al, 2013, s. 103-105). Ikke minst gir denne metodetilnærmingen muligheten til å ta tak i spennende utsagn, og gå dypere inn på interessante meninger eller saker intervjuobjektet snakker om, i en såkalt boreteknikk (Gentikow, 2005, s. 40).

3.2. Kvalitativ metode

Kvalitative data er informasjon det ikke er mulig å kvantifisere i absolutte tallstørrelser, eksempelvis holdninger til et gitt emne eller fenomen. I bruken av kvalitative metoder blir ikke virkeligheten studert som et noe objektivt man kan kvantifisere, men heller noe som er konstruert av sosiale, historiske og individuelle livssituasjoner. Derfor må kvalitativ empiri fortolkes, før den settes inn i kontekst for å gi mening. (Sander, 2021)

Kvalitative intervjuer har, ifølge Østbye et.al (2013) fått en helt sentral plass når det gjelder forskning på publikum (s. 103). Denne metodetilnærmingen kan blant annet gi informasjon det ellers ville vært vanskelig å få tilgang til, og det åpner for å prøve ut egne hypoteser og forståelsesmåter underveis i intervjuet (Østbye, et.al, 2013, s. 103). Det er gjerne tre typer kvalitative intervjuer man skiller mellom. De ulike typene skiller mellom ulike grader innhold og rekkefølge på spørsmålene, og ikke minst hvor strengt man holder seg til disse (Østbye, et.al, 2013, s. 104).

Den første intervjuformen kalles *ustrukturerte intervjuer*. Disse er ofte uformelle, med lite definerte spørsmål på forhånd. Dette kan være en god intervjumetode om forskeren undersøker forhold han eller hun har lite oversikt over, og resultatene kan da bli brukt som grunnlag for mer strukturerte intervjuer (Østbye, m.fl, 2013, s. 104-105). Jeg valgte bevisst å ikke benytte meg av denne intervjumetoden, da jeg følte jeg hadde kunnskap på forhånd, og ville ikke risikere at samtalen sporet av, vekk fra problemstillingen.

Den andre intervjumetoden kalles *semistrukturerte intervjuer*, og her er det et forhåndhåndsbestemt tema det skal stilles spørsmål om. I tillegg er det ofte i denne typen intervju utarbeidet en intervjuguide i forkant, slik at man har enkelte spørsmål å forholde seg til (Østbye, m.fl, 2013, s. 105). Likevel åpner et semistrukturert intervju for høy grad av fleksibilitet, da man kan stille oppfølgingsspørsmål som viker fra intervjuguiden, om informanten kommer med spennende innspill (Østbye, et.al, 2013, s. 105). Jeg har valgt å benytte meg av semistrukturert intervju, da jeg ønsket at intervjuguiden skulle fungere som en pekepinn på hvilken retning intervjuet skulle ta, i tillegg til å ha nok fleksibilitet og mulighet for at informanten kan la tankene gå litt av seg selv og snakke relativt fritt.

Den tredje og siste intervjumetoden er *strukturerte intervjuer,* som gir intervjueren mulighet til å stille forhåndsbestemte spørsmål til informanten, med åpne svarmuligheter (Østbye, et.al, 2013, s. 105). Denne typen intervju kan gjøre det lettere å fremstille svarene i tabeller, ettersom spørsmålene gjerne stilles med utgangspunkt i et skjema (Østbye, et.al, 2013, s. 105). Jeg valgte å gå bort fra denne typen intervju fordi jeg ønsket en åpen dialog og flytende samtale med informantene. Jeg var redd et strukturert intervju kunne ført til at spennende utsagt og tanker kunne forbli usagt, dersom jeg holdt meg strengt til et skjema. Jeg ønsket en intervjusituasjon hvor jeg kunne spille videre på informantenes svar, og gå frem og tilbake til intervjuguiden som en sjekkliste som sørget for at alle spørsmål ble besvart.

3.3. Prosjektets rammebetingelser

Prosjektet er utarbeidet etter tydelig rammebetingelser, både med tanke på tid og kompetanse.

Prosjektet er utarbeidet etter en tydelig *tidsplan*. Dette har gjort et såpass omfattende prosjekt håndterbart, ved at det hele tiden har vært klare rammer på hva som er i fokus i den aktuelle tidsperioden. Et stort prosjekt og et helt studieår til disposisjon kan gjøre det utfordrende å disponere tiden, så en nøye utarbeidet tidsplan med hjelp fra veileder har gjort at det har vært et kontinuerlig driv og fremdrift i prosjektet fra start til slutt.

Kompetanse har også vært en avgjørende faktor i flere av de metodiske valgene. Valg av metodisk tilnærming er først og fremst basert på oppgavens problemstilling, men eget kompetansenivå har også vært en faktor. Som det største forskningsprosjektet jeg til nå har gjennomført, virket det mer hensiktsmessig å velge den metodiske tilnærmingen jeg både behersker best, og synes er en fornøyelse å jobbe med.

3.4. Utforming av problemstilling

I utgangspunktet ønsket jeg å undersøke hvor bevisste mennesker er på data som er lagret om dem, men etter nærmere vurdering fant jeg ut at en slik problemstilling ville være vanskelig å konkludere. I tillegg er det et svært omfattende spørsmål, med mange utfordringer. For å kunne plassere svarene i forhold til hva som faktisk blir lagret, ville jeg vært nødt til å bruke mye tid og ressurser for å få en viss oversikt over innsamlet data, og dette kunne fort vist seg å bli for omfattende for en masteroppgave. Jeg jobbet derfor utfra temaet personvern og overvåkingskapitalisme. Jeg har valgt å fokusere utelukkende på smarthøyttalere. Til tross for at dagens smarttelefoner også er utstyrt med talestyrt smartassistent, anser jeg det som en vesentlig forskjell på å ha en assistent integrert i telefonen, og det å ha installere en IPA i hjemmet, med den hensikt å benytte seg regelmessig av den stemmeaktiverte tjenesten.

3.5. Utforming av intervjuguide

Intervjuguiden er utformet både på norsk (vedlegg A) og engelsk (vedlegg B). Intervjuguiden er basert på de analytiske dimensjonene presentert tidligere, og spørsmålene er utformet utfra teoretiske perspektiver presentert i teorigjennomgangen. Likevel er rekkefølgen på spørsmålene lagt opp etter hvordan jeg følte det ble mest flyt etter fullførte pilotstudier.

Intervjuguiden er delt opp i totalt seks deler, med 3-6 spørsmål i hver del. Det å bygge opp intervjuguiden på denne måten, gjorde det enkelt å la samtalen få en naturlig flyt, og samtidig holde samtalen innenfor gitte rammer. Det var enkelt å få en oversikt over hvilke spørsmål jeg måtte stille, og hvilke spørsmål informanten selv kom inn på. En slik balanse gjør at samtalen er strukturert og har et formål, samtidig som den beholder dynamikken, spontaniteten og flyten til en «vanlig» sosial samtale (Gentikow, 2005, s. 88). Intervjuguiden ble delt opp i følgende kategorier:

Generelt. Denne kategorien ble benyttet for å få samtalen i gang på en naturlig og uformell måte, og har derfor noen flere spørsmål. Her lot jeg deltakerne snakke om hvorfor de kjøpte en IPA, hvor den er plassert, hvor ofte de bruker den, og hva de ser på som fordeler og ulemper med en slik enhet.

Personvern og overvåking. Denne kategorien utforsker informantens syn og holdninger til personvern og overvåking, hvor viktig det er for dem, og hvilke data anser som sensitive.

Personvern, IPA og reklame. Denne kategorien er mer direkte rettet mot IPA-systemer, data de samler inn, og informantenes kjennskap til dette. Her blir også informantene spurt om målrettet reklame og triggerord.

Tanker og refleksjoner. Denne kategorien utforsker informantenes egne historier rundt IPA, og hvorvidt de har opplevde noe ukomfortabelt i forbindelse med assistenten. I tillegg blir temaer som hacking og menneskelig avlytting tatt opp, da det viste seg under pilotstudiene at det fikk en fin flyt.

Aksept. Denne kategorien utforsker informantenes holdninger til ny teknologi. Her innhentet jeg informasjon om blant annet hvorfor de valgte å kjøpe en IPA, og hvor enkelt informantene synes det er å bruke enheten i hverdagen.

Avsluttende refleksjoner. Den siste kategorien tar for seg informantenes holdninger til leverandøren bak sin IPA, og hvorvidt de stoler på leverandøren. I tillegg blir informantene spurt om hva som skal til for at de velger å koble sin IPA ut/inn igjen. Det siste spørsmålet

fungerte utmerket som et avsluttende spørsmål hvor informantene virkelig fikk reflektert over egne grenser hva gjelder personvern og overvåking.

3.6. Erfaringer etter pilotstudiene

Pilotstudier er en utprøving av planlagte metoder i en studie (Braut, 2020). Jeg gjennomførte to pilotstudier. Det første med en svært erfaren informant som har utdanning og jobb innen IT. Denne informanten har derfor mye kunnskap innenfor de teknologiske systemene en IPA benytter (AI og IoT). Det andre pilotintervjuet var med en informant som kjenner til den type teknologi kun fra privat bruk.

Disse to pilotstudiene ble gjennomført for å se hvordan informanter av ulikt kjønn, og med ulik bakgrunn, tolket spørsmålene. Begge pilotstudiene ble gjennomført med norske informanter. Dette var fordi det viste seg å være utfordrende å få tak i nok amerikanske informanter, noe som gjorde at jeg ønsket å være sikker på at intervjuet ble brukbart når det først ble gjennomført. I tillegg var det vanskelig å kommunisere effektivt med amerikanske informanter på grunn av tidsforskjeller, noe som ville gjort det vanskelig å gjennomføre flere intervjurunder under pilotstudiene, dersom det hadde vært nødvendig.

Etter pilotstudiene ble det gjort viktige endringer. Intervjuguiden som tidligere hadde vært kategorisert etter teori, ble forlatt til fordel for temafokuserte kategorier. Dette gjorde at samtalen fikk bedre flyt. Kategoriene ble endret til hvordan jeg oppfattet at informantene fikk delt mest mulig under intervjuet, og samtalen gikk naturlig fra den ene til den andre kategorien. Jeg ønsket å ha flere kategorier med få spørsmål, slik at jeg kunne fokusere på hva informanten sa, fremfor å fokusere på hva neste spørsmål på listen var. Når intervjuguiden ble designet på denne måten var det lett å få en oversikt over hvor jeg burde stille oppfølgingsspørsmål, og hvor jeg fikk tilfredsstillende svar.

Jeg fant ut etter pilotstudiene at det ikke var behov for å legge til så mange nye spørsmål, men heller justere på enkelte formuleringer, og fjerne overflødig spørsmål som ble besvart gjennom andre spørsmål. I tillegg ble det gjort endringer i strukturen. Det viste seg å være utrolig viktig å ha flere kategorier med få spørsmål, slik at samtalen fikk god flyt, samtidig som de viktigste spørsmålene ble besvart.

3.7. Informantutvalg

Kvalitative undersøkelser baserer seg som regel på små utvalg på mellom 1-30 personer (Sander, 2021). Det er likevel anbefalt å ha minst ti informanter i en kvalitativ undersøkelse (Gentikow, 2005, s. 77) I dette prosjektet har jeg totalt 11 informanter; 6 fra Norge og 5 fra USA. I utgangpunktet skulle det være også 6 informanter fra USA, men dette ble ikke mulig. Jeg vil komme tilbake til hvorfor senere i kapittelet om utfordringer. Utvalgskriteriene for informantene er at de er i 20-årene og har en IPA i hus. Jeg har valgt denne aldersgruppen fordi de er hyppig brukere av IPA (Kinsella, 2019). I tillegg er dette en aldersgruppe som, etter mine antakelser, har god erfaring og er åpne for å ta i bruk nye teknologiske systemer. Dette er også mennesker som er voksne nok til å kunne reflektere rundt utfordringer i forbindelse med personvern og overvåking. Ettersom rekrutteringen har skjedd gjennom eget nettverk, har det også gjort det lettere å få tak i informanter i egen aldersgruppe.

3.7.1. Rekruttering

Fra tidligere studier har jeg erfaring med at det kan være utfordrende å engasjere fremmede til å stille opp ved å poste et innlegg på sosiale medier. Jeg benyttet meg derfor av eget nettverk, spurte venner og bekjente om de kjente noen som hadde en IPA, og tok så direkte kontakt med vedkommende, noe som viste seg å være effektivt. Jeg fulgte samme fremgangsmåte både i Norge og USA. Jeg har selv bodd i USA, og benyttet meg av eget nettverk til å komme i kontakt med informanter, i tillegg til at jeg benyttet min søsters og en venninnes nettverk. På denne måten kom jeg i kontakt med mennesker fra hele USA.

Et par av informantene i USA svarte ja til å stille opp til intervju, men da jeg forsøkte å avtale tid fikk jeg ikke lenger svar. Flere dager senere, og etter gjentatte meldinger fra min sine, måtte jeg finne på noe annet. Jeg postet derfor et innlegg på nettforumet Reddit, da jeg visste det fantes egne forum for smarthjem. Jeg postet et innlegg hvor jeg sa jeg lette etter amerikanske informanter i 20-årsalderen med en IPA, som kunne tenke seg å stille til intervju. Jeg fikk da svar fra én person, og vi fikk gjennomført intervjuet dagen etter.

Ingen av informantene ble honorert, og alle stilte opp frivillig. Jeg opplevde det slik at de fleste informantene syntes det var et interessant tema, og noe de gjerne ville snakke om, og dele sine erfaringer rundt. Etter intervjuene var det flere informanter som gjerne ville fortsette å prate om nettopp personvern og overvåking, og flere spennende detaljer viste seg å komme

av denne samtalen etter intervjuets avslutning. Informantene fikk da spørsmål om det var i orden at jeg benyttet meg av deres refleksjoner og enkelte sitater som kom frem etter at intervjuet i utgangspunktet var avsluttet, noe samtlige samtykket til.

3.7.2. Beskrivelse av informantene

I denne tabellen er en kort beskrivelse av informantene. Deres ekte navn er byttet ut med et pseudonym.

Norske informanter:

Navn	**Kjønn**	**Alder**	**Land**	**Type IPA**
Thomas	Mann	29	Norge	Amazon Alexa
Mina	Kvinne	24	Norge	Google Home
Eirik	Mann	26	Norge	Google Home
Sara	Kvinne	29	Norge	Amazon Alexa
Ole	Mann	26	Norge	Google Home
Sander	Mann	21	Norge	Google Home

Amerikanske informanter:

Navn	**Kjønn**	**Alder**	**Land**	**Type IPA**
Rachel	Kvinne	24	USA	Google + Alexa
Taylor	Kvinne	24	USA	Amazon Alexa
Josh	Mann	26	USA	Google Home
Brian	Mann	24	USA	Google Home
Michael	Mann	28	USA	Amazon Alexa

3.8. Digitale utfordringer

Det har oppstått flere utfordringer i forbindelse med koronapandemien, men jeg vil også tørre å påstå at det har gitt muligheter jeg ikke ellers ville hatt. Da jeg gikk i gang med intervjuer i desember 2020, var det strenge sosiale koronarestriksjoner, noe som gjorde at alle intervjuer måtte gjennomføres digitalt. Jeg var redd dette ville ødelegge mye av flyten i samtalen, og gjøre at informantene kanskje helst ville svare så kort og raskt som mulig, for å bli fort ferdig. Av egen erfaring synes jeg det kan være vanskelig å opptre like avslappet, utadvendt og naturlig i digitale møterom, og jeg var redd dette ville påvirke intervjusituasjonen. Etter å ha gjennomført pilotintervjuene, merket jeg derfor fort hvor viktig inngangen til intervjuet var.

Det var viktig å få i gang samtalen på en avslappet, uformell måte, slik at begge parter ble komfortable med å gjennomføre intervjuet digitalt. De aller fleste var også vant til hjemmekontor på denne tiden, og mange hadde, på grunn av pandemien, fått god erfaring med digitale møter, noe jeg tror var en stor fordel.

En annen utfordring med slike digitale intervjuer, er informasjonsskrivet. Digitale møter kan avtales på svært kort tid, og jeg opplevde en utfordring med å sende informasjonsskrivet til informanten i god tid før intervjuet, be dem skrive det ut, signere, scanne inn og sende tilbake til meg. Plutselig ble en enkelt signatur en stor jobb for informanten, noe jeg ser på som en stor ulempe. Disse menneskene stilte opp frivillig, og jeg ønsket ikke at deres generøsitet skulle gi dem ekstra arbeid. Derfor valgte jeg heller å gå over til muntlig samtykke. Jeg startet hvert intervju med å lese opp informasjonsskrivet, hva studien handler om, hvordan data ville bli samlet inn, hvordan deres opplysninger ville bli håndtert, deres rettigheter, dato for sletting av personlig opplysninger og hvem de kunne kontakte dersom de ønsket å trekke seg fra studien. Deretter ga de sitt muntlig samtykke. Jeg gikk i gang med muntlig samtykke så fort jeg fikk godkjennelse av veileder.

Noe jeg ser på som en stor mulighet med tanke på koronapandemien, og de strenge restriksjonene, er hvordan grunnlaget for de norske og amerikanske informantene plutselig ble helt likt. Hadde det ikke vært for pandemien, ville trolig alle de norske intervjuene blitt gjennomført i person, og ikke digitalt. Dette kunne gitt de norske informantene større muligheter til å gjennomføre intervjuet på en mer avslappet og naturlig måte, mens de amerikanske ville kanskje vært preget av utfordringene jeg beskrev tidligere. Når alle informantene hadde samme utgangspunkt gjorde det at jeg kunne se på alle innsamlede data med samme øyne. Alle hadde samme forutsetninger og utfordringer, og de ble løst på akkurat samme måte.

En annen positiv side var hvordan de digitale møtene sparte både meg og informantene for mye tid. Jeg kunne si til informantene at det tok mellom 45 minutter og en time, og det var nettopp det det gjorde. Det krevde ingen tid til å finne et passende møterom, sette opp utstyr og passe på avstand. Alt kunne gjøres klart på forhånd, og være over på den tiden de hadde satt av.

Jeg opplevde dog at intervjuene med de amerikanske informantene gikk mye fortere i forhold til de norske, til tross for at spørsmålene var akkurat de samme. De norske intervjuene tok 45-60 minutter, mens samtlige av de amerikanske intervjuene var ferdig på omlag 30 minutter. Jeg tror dette kan skyldes språkforskjeller. Til tross for lite utfordringer hva gjelder språket i seg selv, så opplevde jeg det slik at amerikanske informanter ikke var like glad i småprat som hva de norske informantene var.

3.8.1. Øvrige utfordringer

En annen utfordring er at et par av informantene hadde koblet ut sin IPA nylig. Det var ikke noe som ble opplyst om i forkant av intervjuet. Grunnen er trolig at jeg ikke opplyste om at det var et kriterium for informanter at deres IPA sto koblet i per dags dato. Da jeg så at dette gjaldt flere av informantene valgte jeg å likevel inkludere dem i analysen. Det var relevant å se på hvorfor informantene har valgt å koble den ut, og hvorfor noen har valgt å beholde den påkoblet.

3.9. Etikk

Jeg vil nå se nærmere på etiske hensyn det er viktig å ta stilling til i en kvalitativ datainnsamling, og hvordan jeg har valgt å løse disse i forhold til oppgaven. Prosjektet er registrert og godkjent RETTE (vedlegg C), etter avtale med veileder. RETTE er UiBs kontrollsystem for behandling av personopplysninger i forskningsprosjekter (UiB, 2019).

Som forsker er man nødt til å operere med informert samtykke, og man bør gjøre det umulig å spore sitater tilbake til personen (Østbye et.al, 2013, s. 131) Informantene i denne studien har alle gitt sitt samtykke, etter å ha fått presentert informasjonsskriv rundt studien, og hva det vil innebære for dem å delta. På grunn av pandemisituasjonen, og det faktum at alle intervjuer ble gjennomført digitalt, ble et slikt muntlig samtykke drøftet og avklart med veileder, og det viste seg å fungere godt.

Ifølge Østbye et.al (2013, s. 131), er det viktig at personer ikke kan identifiseres på bakgrunn av opplysninger som kommer frem i studien. Jeg har valgt å tildele hver informant et pseudonym (fiktivt navn), og presenterer alle informantene i et skjema sammen med deres alder, kjønn, land og hvilken type IPA de eier. Dette er kun informasjon som er relevant for oppgaven.

De som blir forsket på har krav på at informasjonen de gir til intervjueren blir behandlet med respekt og konfidensialitet. Forskeren må forhindre bruk og formidling av informasjon som kan skade enkeltpersoner (Østbye m.fl, 2013, s. 132). I studien har all personlig informasjon blitt lagret separat, for å ivareta informantenes personvern. Lydopptak fra intervjuet har blitt lagret med en navnekode, og oppbevart på en ekstern enhet. Navnekoden har blitt linket til pseudonymet på en annen ekstern enhet, og øvrig informasjon som linker personen til pseudonymet er lagret på en tredje ekstern enhet.

Et siste viktig punkt innenfor etiske hensyn, er forskerens rolle. Når forskeren presenterer sin forskning, representerer han eller hun ikke bare seg selv, men også forskningsinstitusjonen (Østbye m.fl, 2013, s. 132). Dette har jeg vært nødt til å ta særlig stilling til i enkelte av intervjuene. Noen av informantene er mennesker jeg har et personlig forhold til, noe som kan gjøre det mer utfordrende i en intervjusituasjon, hvor man inntar andre roller enn hva man er vant med. Det har i disse situasjonene vært viktig for meg i ivareta min rolle som forsker og intervjuer, og ikke venn eller bekjent. Dette har jeg sett på som viktig for å unngå at informantene deler informasjon med meg som privatperson, og ikke meg som intervjuer og forsker, og dermed kanskje risikere at informantene i etterkant sitter med en følelse av at de delte for mye, og i verste fall risikere at de ønsker å trekke seg fra studien.

3.10. Forskningsprosessen

Nå vil jeg redegjøre for valgene tatt underveis i selve forskningsprosessen, gjennomføringen av intervjuene og dataanalysen.

3.10.1. Gjennomføring av intervjuene

Etter å ha gjennomført de to pilotintervjuene valgte jeg å inkludere begge intervjuene i oppgaven. Informantene til pilotintervjuene ble valgt på bakgrunn av deres ulike bakgrunn; en med mye bakgrunnskunnskap, og en med helt alminnelig kunnskap hva gjelder emnet. Begge informanter ga reflekterte, gode og interessante svar, og jeg så det som en fordel å inkludere begge intervjuene i analysen. Pilotintervjuene ble gjennomført i desember 2020, og resterende intervjuer ble gjennomført i januar 2020.

Endringene som ble gjort etter pilotintervjuene, hvor kategorier og spørsmålsrekkefølgen ble tilpasset samtaleflyten, gjorde det enkelt å holde oversikt gjennom intervjuene. Dermed var det lett å gå forbi enkelte spørsmål som informanten allerede hadde svart på, uten at jeg behøvde å stille selve spørsmålet. Det var da lettere å stille oppfølgingsspørsmål om det var noe spesielt jeg trengte informasjon om. Etter at jeg følte jeg var ferdig med en kategori og klar til å gå over til neste, gikk jeg alltid over de spørsmålene innenfor kategorien for å sjekke at det ikke var noen ubesvarte spørsmål.

3.10.2. Transkribering

Å transkribere betyr å konvertere tale til tekst. Transkriberingen gjør det mulig å dokumentere og analysere innsamlet datamateriale (Sander, 2020). Alle intervjuene ble transkribert kort tid etter intervjuet hadde funnet sted. Fyllord som «eh» «hmm» og liknende ble kuttet ut, noe som er anbefalt å gjøre (Gentikow, 2005, s. 117). Jeg valgte i tillegg å kutte ut setninger som avbrøt hverandre. Hvis en informant startet å si noe, men avbrøt seg selv og startet en ny setning valgte jeg å kun ta med det som var den faktiske setningen. Dette ble gjort for å forbedre lesbarheten i selve analysen. Til tross for at det finnes mange programmer som kan konvertere lyd til tekst, valgte jeg å gjøre transkriberingen manuelt, da dette ga muligheten til å gå gjennom lydopptaket flere ganger, noe jeg tror var en fordel i analysearbeidet. Jeg opparbeidet meg god kontroll over intervjuene, og visste hvilke sitater som illustrerte ulike perspektiver.

3.10.3. Analysearbeid

Det første stedet man bør begynne i dekodingen av innsamlet datamateriale, er å lese gjennom alle transkriberinger for å lete etter gjentakende temaer (Alase, 2017). Jeg valgte å ta fatt på analysen ved å printe ut de nærmere 100 sidene med innsamlet datamaterialet, før jeg benyttet meg av markeringspenner i fire forskjellig farger – en for hver analytiske dimensjon. Jeg markerte så alle sitater innenfor hver enkelt dimensjon. Deretter gjorde jeg det samme digitalt, slik at jeg hadde alt materiale kategorisert, både digitalt og i fysisk form. Deretter gikk jeg gjennom hver enkelt kategori, og kategoriserte på nytt. Denne gang så jeg etter gjentakende holdninger, følelser og tanker innenfor den aktuelle dimensjonen, som resulterte i underkategorier i analysen.

På dette tidspunktet, etter å ha lyttet gjennom intervjuet flere ganger, transkribert og kategorisert i flere omganger, hadde jeg såpass god kontroll over sitatene at det var enkelt å gå frem og tilbake for å finne et sitat som illustrasjon i min analyse. I tillegg følte jeg meg trygg på at jeg hadde oppfattet informantene rett, og hadde en god forståelse for hva som ble sagt og ment med forskjellig utsagn.

3.11. Generalisering

Hvorvidt det er nødvendig å generalisere, eller hvordan man skal gå frem for å generalisere kvalitative studier har vært diskutert i lang tid (Tjora, 2017). Thagaard (2003) bruker for eksempel begrepet *overførbarhet* i stedet for, eller synonymt med generalisering. Overførbarhet betyr at den kunnskapen og forståelsen en studie gir, også er relevant i andre, liknende situasjoner, utenom den ene studien (Thagaard, 2003). En studies generaliserbarhet sier noe om hvorvidt funnene som kommer frem, også er gjeldende for andre enn de som deltok i studien (Kvale, 1997). Både forsker og leser er påvirkende faktorer som sier noe om studiens generalisering. Forskeren kan fremlegge argumenter som forklarer hvorfor studien er relevant i andre situasjoner, og leseren kan kjenne seg igjen i situasjoner, temaer og fenomener som trekkes frem i studien (Sommerbakk, 2012).

En måte å generalisere en studies funn på, er utfra en analytisk vurdering (Kvale, 1997). Det er da tatt en vurdering på om en studies funn sier noe om hva som vil skje i en lignende situasjon, basert på en analyse av forskjeller og ulikheter i de to ulike situasjonene. Forskeren presenterer og argumenterer for sine funn, og det blir opp til leseren å vurdere generaliserbarheten (Sommerbakk, 2012).

En annen måte å generalisere en studies funn på, er ved forskergeneralisering (Kvale, 1997). I et slikt tilfelle kan det vurderes om det er forsker eller leser som skal si noe om generaliserbarheten. Forskeren kan argumentere for studiens generaliserbarhet, men leseren kan også trekke slutninger utfra studien, og benytte seg av dem i egne situasjoner, og dette kalles lesergeneralisering (Sommerbakk, 2012).

Denne studien inkluderer kun 11 informanter. Ettersom utvalget er begrenset, er det vanskelig å generalisere funnene. I tillegg er det bare 5 og 6 informanter fra hvert land. Derfor vil jeg ikke tørre å påstå at funnene i denne studien er relevant for andre enn de som deltok. Likevel

er det enkelte oppfatninger og forståelser av ulike begreper eller fenomener som går igjen, og disse funnene blir også forankret i teoretiske perspektiver. På bakgrunn av analytisk vurdering og tolkningen av funn, vil jeg derfor si at det er opp til leseren å vurdere generaliserbarheten. Kanskje øker studien leserens forståelse av overvåking og personvern, og kanskje kommer det frem analytiske funn han eller hun kjenner seg igjen i.

3.12. Begrensninger

Prosjektet er basert på fire analytiske dimensjoner som på hver sin måte belyser problemstillingen. En begrensning i studien er at dimensjonene er såpass store på egenhånd, i tillegg til at prosjektet har tids- og ordbegrensning. Dette gjør at studien ikke undersøker i dybden like mye som den gjerne skulle gjort. Det ville sannsynligvis vært en fordel å omformulere og fokusere på kun overvåking og personvern, da det ville beriket oppgaven med ytterligere dybde, fremfor bredde.

En annen begrensning i prosjektet er studiens validitet. En studies validitet sier noe om studien måler det forskeren faktisk ønsker å måle (Dahlum, 2021). På grunn av språkforskjeller er det en reell mulighet for at informantene, særlig fra USA, har oppfattet spørsmålene forskjellig, og derfor kan jeg ikke være 100% sikker på at studien måler det jeg faktisk ønsker å måle, nemlig informantenes refleksjoner rundt personvern og overvåking i bruken av IPA. I tillegg kan prosjektet bære preg av bias. Dette betyr at den kan bære preg at en ensidig synsvinkel som kan ha påvirket resultatene, og at det kan ha blitt stilt ledende spørsmål til informantene (Grønmo, 2020).

3.13. Oppsummering

Dette kapittelet redegjør for prosjektets metodetilnærming og metodiske valg tatt gjennom prosessen. Jeg har valgt kvalitativ metode fordi jeg ønsker å forstå hvordan unge mennesker i Norge og USA resonnerer rundt personvern og overvåking i bruken av smarthøyttalere. Semistrukturerte intervjuer ble gjennomført med totalt 11 informanter, hvorav 6 er norske og 5 er amerikanske. Etter at alle metodiske valg er redegjort for, vil jeg starte analysen med prosjektets første dimensjon: overvåking.

4. Overvåking

Analysens aller første dimensjon tar for seg hvordan informantene reflekterer rundt fenomenet overvåking. Til tross for at overvåking ikke er et nytt fenomen, har praksisen rundt det endret seg over tid, etterhvert som nye teknologiske enheter har blitt implementert i prosessen (Lyon, 2006, 3). Overvåking kan defineres som *systematisk,* fordi informasjonen som samles inn ikke er tilfeldig, *fokusrettet,* fordi oppmerksomheten er rettet mot enkeltpersoner, og *rutinemessig,* fordi det oppfattes som en normal del av hverdagslivet (Lyon, 2007, ss. 14-15). Sannsynligvis har du på et eller annet tidspunkt tatt i bruk teknologi for å holde øye med noen andre, og det behøver nødvendigvis ikke være noe dumt i det. Eksempelvis kan dette være å sjekke kartfunksjon på sosiale medier, for å sørge for at venninnen din har kommet seg trygt hjem. Det kan være å installere en app på barnets telefon for å holde et øye med dem, eller jobbe som vekter, og passe på at det er ro og orden gjennom overvåkningskameraer. Denne type overvåking er som oftest basert på omsorg for de rundt deg, og har en ærlig hensikt. Men de teknologiske enhetene vi stadig gir større rom til i en digitalisert hverdag kan også åpne opp for overvåking fra store selskaper med en bakenforliggende hensikt: økonomi. Med IPAer som kjenner til vanene våre, søkehistorikken, stemmen og tonefallet vårt, skaper det en sømløs og personlig service som konstruerer et forhold mellom bruker og selskap. Men det er også en tjeneste som åpner dørene for overvåking i flere private rom og situasjoner. (West, 2019)

4.1. Holdninger til overvåkingsfenomenet

Aller først vil jeg analysere informantenes holdninger til fenomenet overvåking. Informantene ble derfor bedt om å reflektere over hva begrepet overvåking betyr for dem, og hvilke assosiasjoner de forbinder med ordet. Majoriteten av informantene anser begrepet overvåking som et negativt laget begrep, og assosierte det med noen eller noe som er ute etter å samle inn informasjon om deg. Sander på 21 år forbinder overvåking med noen som er ute etter ens informasjon, og at de går aktivt inn for å få tak i den:

> Jeg tenker at overvåking er at noen skal finne ut informasjon om deg. Og at de går inn for å gjøre det. Det er jo litt sånn hvis noen hacker meg og hører på hva jeg sier i huset, eller når jeg er hjemme, over telefonen og sånne ting. At noen skal på en måte skal ha min informasjon og bruke den til noe da, eller bli kjent med hva jeg gjør eller driver med. (Sander)

Sanders refleksjoner rundt overvåking har en noe negativ undertone, og han nevner hackere som en potensiell trussel. Hans definisjon har likhetstrekk med Lyons beskrivelse av fenomenet, hvor innsamlingen av informasjon er både fokusrettet og systematisk (Lyon, 2007, ss. 14-15). Sander nevner ikke hvorvidt han mener overvåking skjer med eller uten *samtykke,* men det kan tolkes som at hans generelle oppfatning av fenomenet er noe som skjer uten samtykke, da han nevner hackere, som vanligvis operer uten tillatelse fra sine ofre. Rachel på 24 år mener overvåking ofte skjer uten tillatelse, men at det kan innebære begge deler. Hun oppfatter fenomenet som ubehagelig og ekkelt:

> Surveillance I would say, is when you´re being watched or listened to. With your permission or not. I feel like when you´re being surveilled it's kind of like, not with your consent. It is kind of like a creepy term, I don't know. It's weird. (Rachel)

Rachel nevner ikke eksempler på hvem som potensielt kan stå bak denne overvåkingen, slik Sander gjør. Hun ble derfor stilt et oppfølgingsspørsmål om hvem eller hva hun sikter til, og ifølge Rachel er det en frykt for overvåking fra selve IPAen hun anser som ubehagelig:

> I think the speakers are listening constantly, and some of them are connected to say Amazon, and other things. And I'll be talking about something, and get like, on my phone, I´ll get like an ad or something that I was talking about, and it is just creepy. (Rachel)

Den overvåkingen Rachel beskriver her, hvor hun kan snakke om et produkt og deretter få målrettede annonser, er hva Zuboff beskriver som overvåkingskapitalisme (2019). Rachel tror IPAen lytter konstant til hennes samtaler, og synes det er ekkelt. Ifølge Amazon skal ikke mikrofonen bli aktivert før triggerordet til assistenten er sagt, men dette har tidligere vist seg å ikke alltid være tilfelle (Wolfson, 2018). For et selskap som Amazon vil *tillitt* mellom forbruker og selskap trolig være et viktig nøkkelpunkt for hvor mye deres kunder er villig til integrere deres produkter i livene sine, og hvis flere forbrukere er av den oppfatning at deres IPA lytter konstant, kan dette ha en negativ effekt på fremtidig bruk. Også 29 år gamle Sara trekker frem det Zuboff beskriver som overvåkingskapitalisme som noe negativt i forhold til overvåking, og tar sterk avstand fra informasjonsinnhenting med markedsføringsformål:

> Jeg synes ikke overvåking og informasjonsinnhenting er greit i markedsføring. Fordi det er ikke en fare, det er bare for å innhente så mye informasjon som mulig, sånn at de kan tilpasse reklame. Det synes jeg ikke er greit, det er bare griskhet. (Sara)

Sara tar altså sterk avstand fra overvåking til markedsføringsformål, men mener likevel det er mulig å bruke overvåking til noe positivt, hvis situasjonen tilsier det, til tross for at det er frihetsbegrensende:

> Overvåking er en begrensning av frihet på en måte. Men jeg tenker det kan være både positivt og negativt. Hvis man er i en tidsperiode hvor det er stort trusselbilde, så er man kanskje mer villig til å gi opp mer av friheten sin, for eksempel ved at man blir overvåket i hjemmet. Hvis det er en overhengende fare for at noe kan skje, så tror jeg de fleste ville sagt seg enig for å beskytte seg selv og de rundt. (Sara)

For Sara handler altså overvåking om konteksten, og til hvilket formål overvåkingen blir brukt til. For 26 år gamle Ole er begrepet overvåking negativt ladet, men i likhet med Sara mener han det er i orden å bli overvåket hvis situasjon tilsier det. Sara mener dog at overvåkingen kan også skje i hjemmet hvis det er stort trusselbilde. Ole derimot, tar sterk avstand fra all type overvåking i hjemmet, og forklarer det slik:

> Overvåking er jo negativt ladet, men det er jo bra noen steder. Jeg tenker det er viktig der hvor ting kan skje og hvis det er viktig å dokumentere hvem som har gjort hva. Men sånn i hjemmet, så synes jeg ikke det er greit. Da tenker jeg på all overvåking, både fra andre mennesker og teknologi. Hvis noen hadde satt opp et kamera hjemme hos meg for eksempel, så hadde jo ikke det vært greit. (Ole)

26 år gamle Josh forbinder overvåking med noe som skjer når man er ute i offentlig rom, hvor man sannsynligvis blir filmet av én eller flere enheter. Han mener derimot at overvåking ikke nødvendigvis er en negativ ting, men at det har potensiale til å bli misbrukt:

> I guess I always consider surveillance from a public perspective, and it's the idea that when you're in a public space you're probably being watched by one thing or another. Your government, or private security cameras that you walk by on the street, and I don't think that surveillance is necessarily a bad thing, but I do think that it has the potential to be misused. (Josh)

Josh ser altså overvåking fra et litt annet perspektiv enn de andre informantene, som trekker frem hackere og selskaper som er ute etter personlig informasjon. Josh på sin side ser overvåking fra et offentlig perspektiv, hvor statlig overvåking eller private overvåkningskameraer er å forvente. Han mener denne formen for overvåking ikke

nødvendigvis er en negativ ting. Josh definerer altså fenomenet overvåking på en litt annen måte enn hva Lyon (2007, ss. 14-15) gjør, ettersom den typen overvåking Josh forholder seg til, ikke nødvendigvis er fokusrettet eller systematisk. Han opplever det dog som *rutinemessig*, og en del av hverdagen.

Informantene deler altså den oppfatningen at overvåking er når noe eller noen forsøker å få tak i informasjon om deg, og flere trekker frem at det er negativt ladet begrep, eller at de har negative assosiasjoner til fenomenet. Likevel blir det trukket frem situasjoner hvor overvåking kan ha en positiv effekt, og terror blir brukt som eksempel fra flere av informantene. I informantenes refleksjoner rundt overvåking som fenomen kommer det frem lite kulturelle forskjeller, og det er ingenting som tyder på at det er forskjellig oppfatning av overvåking basert på kjønnsforskjeller. Men alder ser dog ut til å spille en rolle akkurat her. Informantene som er 25 år og yngre trekker *ikke* frem overvåking som et positivt hjelpemiddel i enkelte situasjoner, noe alle over 25 år gjør, hvor da terror og stort trusselbilde blir nevnt. Dette blir naturligvis spekulasjon, men en mulig årsak kan for eksempel skyldes at informantene over 25 år i større grad husker terrorangrepet 9/11, og 22 juli sitter muligens sterkere i minne for de norske informantene som var eldre da angrepene skjedde. Det er nemlig mange som forbinder 9/11 med startskuddet for overvåking, og det er ikke helt feil. Det offisielle målet for å etablere overvåkingssystemer var nemlig kampen mot terrorisme og organisert kriminalitet, men den egentlig utviklingen begynte lenge før det, og flere overvåkingssystemer var allerede implementert da angrepene skjedde (Mathiesen, 2013, s. 63). Likevel kan alder, og et sterkere minne av 9/11 være en faktor for hvorfor informantene over 25 i større grad trekker frem terror og den positive innvirkningen overvåking kan ha i slike tilfeller.

4.2. Tjuvlytter du, Alexa?

Etter å ha kartlagt informantenes generelle holdninger til fenomenet overvåking, vil jeg nå se nærmere på deres holdninger til IPA-systemet. Informantene ble spurt om hva de anser å være IPAens største fordel. Her svarte de aller fleste av stemmestyring var IPAens største fordel, etterfulgt av pris og bekvemmelighet. Når de ble spurt om største ulempe var det stor forskjell mellom norske og amerikanske informanter. Med unntak av én, sier alle informantene fra Norge at de ser på avlytting og overvåking som den største ulempen, mens den siste informanten fra Norge nevner at det er skremmende når IPAen snakker av seg selv. Derimot

er det kun én informant fra USA som nevner overvåking som en ulempe. I skjemaet under blir det presentert i korte stikkord hva informantene ser på som IPA-ens mest negative side.

Navn	Land	Største ulempe med IPA
Thomas	Norge	• Overvåking • Snakker av seg selv
Eirik	Norge	• Skremmende når den snakker av seg selv
Ole	Norge	• Kanskje blir avlyttet hele tiden
Sander	Norge	• Vet ikke om den avlytter
Mina	Norge	• Hvis den avlytter, og samler informasjon
Sara	Norge	• Føler seg overvåket
Josh	USA	• Eldre funksjoner som ikke lenger blir oppdatert eller støttet.
Brian	USA	• Har liten nytte om man ikke har smart-hjem
Michael	USA	• Avhengig av internett, som ofte er ustabilt under orkan-sesong
Rachel	USA	• Avlytting
Taylor	USA	• Kobler seg av og til fra internettet

De norske informantene er langt mer kritiske til IPAens evne til å overvåke, i forhold til de amerikanske. Rachel, som forklarte overvåkingsfenomenet som at noen ser eller hører hva du driver med, gjerne uten samtykke, er den eneste amerikanske informanten som trekker frem avlytting som IPAens største ulempe, og forklarer det slik:

> I really do think they are listening to us, for sure. (Rachel)

Med unntak av amerikanske Rachel, frykter altså de norske informantene overvåking fra IPAen i større grad enn hva de amerikanske gjør. I tillegg er det forskjell på hva informantene er redd for i forbindelse med overvåking fra assistenten, noe jeg vil gå dypere inn på nå.

4.2.1. «Du har snakket om terror, du kan være terrorist.»

Av informantene som svarte at de anså overvåking og avlytting som den mest negative siden ved en IPA, er det særlig én ting flere informanter nevner som bygger på frykten for overvåking. Nemlig det å si noe «feil» i sitt eget hjem foran IPAen, og havne i politiets søkelys. Sara endte med å koble sin assistent ut:

> Jeg syntes det var så ubehagelig at den sto på hele tiden, så jeg koblet den ut til slutt. Siden den lyttet hele tiden, så var jeg litt redd for å si noe som den kunne tolket feil. Man har jo ikke så mye filter i sitt eget hjem, og snakker jo om løst og fast. (Sara)

For Sara var altså følelsen av å ikke kunne snakke fritt i hjemmet sitt, nok til at hun valgte å koble ut sin IPA. Til tross for at hun ikke har noe å skjule, synes hun det var ubehagelig å ikke vite hva assistenten plukket opp, og hvordan ting kunne blitt tatt ut av kontekst:

> Si man snakker om bomber da, så tar den opp ord, og plutselig får man noen som lytter til deg, sånn politiet eller noe sånt. Jeg har jo ikke noe å skjule, men det er jo veldig uheldig om den plukker opp ord og tar de ut av kontekst, og plutselig blir man undersøkt. (Sara)

Overvåkingen Sara frykter mest er altså en overvåking fra politiet, dersom IPAen plukker opp triggerord og utløser en alarm. Hun beskriver denne frykten som å ha en person sittende i hjemmet:

> Jeg var redd for å si ting etter hverandre for å trigge noe slags overvåking. Jeg tror veldig mange har samtaler hjemme som absolutt ikke er noe farlig, men som man kanskje ikke ville snakket om utenfor huset da, og jeg bare synes det er ekkelt med en sånn høyttaler. Det er jo som at man har en person sittende i stua. (Sara)

For Sara, som tidligere fortalte at hun var åpen for overvåking i situasjoner hvor trusselbildet er høyt, er samtidig redd for å bli utsatt for en skjult overvåking i hjemmet, hvor ord kan bli tatt ut kontekst og gjøre henne selv til en mistenkt. Også 24 år gamle Mina, nevnte det å ha en slags frykt for å snakke om sensitive temaer som noe hun hadde reflektert rundt, og beskrev dette eksempelet som skremmende:

> Jeg og kjæresten min snakket om fascisme, og vi var dypt inne i samtaleemnet da Google Home avbrøyt oss og sa *«dette er hva jeg fant på internett om Interpol».* Da føltes det ut som hun hadde

> vært med gjennom hele samtalen, og avbrøyt oss i form av en varsel som at *«hei, jeg hører på hva dere sier».* (Mina)

Mina ble altså avbrutt av sin IPA midt i en samtale om fascisme, med informasjon om internasjonalt politi, noe som gjorde at hun også valgte å koble ut sin IPA:

> Min umiddelbare reaksjon var jo å le og bare hva faen liksom. Men når vi fikk latt situasjon senke seg litt, og fikk reaksjonen litt på avstand, så var det litt sånn *«kanskje vi burde trekke ut kontakten».* (Mina)

Å snakke om terror i hjemmet er også noe som blir nevnt av Ole, som beskriver det på følgende måte:

> Si man snakker om terror hjemme da. Så plutselig registrerer den at vi snakker om terror, så registrerer den inn til en eller annen liste, at *«du har snakket om terror, du kan være terrorist».* (Ole)

Det å ha en reell frykt for å havne i politiets søkelys er noe som har blitt beskrevet av flere norske informanter, men ingen amerikanske. På den andre siden var det flere norske informanter som selv trakk frem at de ville vært positive til overvåking, dersom det er for egen og andres sikkerhet. Overvåking, eller frykten for overvåking ser med andre ord ut til å være skremmende effektiv, og det er noe flere av informantene forholder seg til. Sara forklarer hvordan hennes frykt for å si noe feil i eget hjem, har gjort at hun ikke lenger ønsker å bruke sin IPA. Det kommer ikke frem i intervjuene *hvorfor* flere norske informanter er av den oppfatning at politiet uten videre kan få tilgang til IPA-opptak, men det ville utvilsomt vært spennende å se nærmere på. Lydopptak fra Amazon Alexa har ved flere anledninger blitt brukt som bevis i drapssaker. Samtidig sa Amazon i 2019 at de ikke svarer på myndigheters krav om kundeinformasjon, med mindre de er lovpålagt å gjøre det for å overholde en juridisk bindende ordre (Burke, 2019). Så til tross for at statlig overvåking er noe flere norske informanter trekker frem, er det ingenting som tyder på at dette blir praktisert.

4.2.2. «Jeg har ingenting å skjule.»

Argumentet om at en ikke har noe å skjule den største gjentakende faktoren hos de som ikke frykter overvåking. Da informantene spurte hvilke tanker de hadde gjort seg opp rundt det at IPAen har en mikrofon som alltid er påkoblet, med mindre de selv velger å skru den av, var svarene to-delt. Flere av informantene var skeptiske til dette, og enkelte hadde valgt å skru av

sin IPA for å ikke føle seg overvåket. Mange er likevel ikke bekymret, da de ikke har noe å skjule. 26 år gamle Eirik er den eneste informanten fra Norge som ikke tar opp overvåking som en negative side ved en IPA, og han beskriver det slik:

> Det er jo sånn, når jeg forteller folk som er mer kritiske til dette at jeg har mye smart-funksjoner i hjemmet, og de kommer jo med den påstanden *«ja, men tenk om de hører hva du sier!»,* da er egentlig argumentet mitt at jeg ikke sier så mye spennende som de kan bruke da. (Eirik)

Eirik spesifiserer ikke hvilken informasjon han ser på som ubrukelig, og hvem som eventuelt skulle ha interesse av denne informasjonen, men det er grunn til å tro at han sikter til leverandøren av smart-funksjonene, som i hans tilfelle er Google. Eirik mener denne informasjonen, som innebærer hans daglig rutiner, ikke har noen verdi. Skal man derimot tro teoretikere som Zuboff (2019), Gandy (2011), og Campbell & Carlson (2002), har denne informasjonen en enorm verdi som sammen kartlegger en person til den minste detalj. Som Gandy (2011) hevder, er ikke hver enkelt bit av informasjon nødvendigvis viktig eller særlig verdifull alene, men verdien skapes når hver ekstra bit med informasjon skaper en profil av en forbruker som tilsammen muliggjør identifisering og klassifisering av individet. Nøkkelen for selskaper er å få tak i den biten med informasjon som løser identifikasjons-puslespillet, som kan resultere i et lite konkurransefortrinn for selskapet (Gandy, 2011, s. 446). Dermed kan den informasjonen Eirik ser på som lite interessant, plutselig være en viktig nøkkelfaktor for leverandør og deres samarbeidspartnere.

24 år gamle Brian deler Eiriks syn på at han ikke føler han har noe å skjule. Grunnen til at han ikke bekymrer seg for overvåking, er fordi han ikke er kriminell, og derfor ikke har noe å skjule. Dette gjør at han ikke bekymrer seg for om hans IPA hører hva han sier, til tross for at han opplevd at den snakker av selv. Han forklarer det slik:

> The microphone never really bothered me. I mean if I was on the run it would definitely bother me, or if I had like a drug run in the background, but like… It didn't bother me, even if it was always listening. (Brian)

Brian har, i likhet med andre informanter, opplevd at IPAen har begynt å snakke uten at triggerordet har blitt sagt, og han vet det er en risiko rundt at uvedkommende kan få tilgang. Likevel er det ikke noe han føler seg skremt av:

> I mean I know they´re always recording, and I think it's really dumb to assume that it's not capable of being accessed by other people. But it doesn't bother me really. It used to turn on all the time and be like *"what was that?",* so you could tell it was listening, but it didn't bother me. (Brian)

28 år gamle Michael legger i likhet med Brian vekt på at han ikke gjør noe ulovlig, og dermed ikke føler at overvåking er noe han bør frykte:

> I just don't quite care. I don't do anything illegal. If they want to check in and see what I'm doing, listen to my conversations, it's like have fun. It's probably just me talking to my friends or watching TV, so.. it's not really anything I'm worried about. (Michael)

Det er tryggheten ved å ikke ha noe å skjule som ser ut til å være den største faktoren hos informantene som ikke frykter overvåking fra sin IPA. Denne begrunnelsen blir kun nevnt av mannlig informanter, og i hovedsak amerikanere, med unntak av én norsk informant. Informantene med denne holdningen trekker også frem kriminalitet. Det at de ikke gjør noe ulovlig gjør at de ikke er redd for overvåking. Andre informanter er derimot redd for å bli oppfattet som kriminelle, uten å være det. Det ser derfor ut til at informantene generelt ikke forstår konseptet rundt kommersiell overvåking, og anser heller overvåking som noe som skjer i forbindelse med terror og kriminalsaker. Det er nemlig ingen som sier de frykter overvåking gjennom IPAen fordi de for eksempel er redde for at kommersielle selskaper skal kjenne til deres vaner og holdninger, og bruke dette til sin fordel.

4.2.3. Hacking

IPA har fått mye kritikk for å være utsatt for hacking. I 2017 hadde fast food-kjeden Burger King en TV-reklame med setningen «OK, Google, tell med about the Whopper burger». Dette skal ha aktivert svært mange Google Home-assistenter, som deretter listet opp alle ingrediensene i den kjente burgeren. Dermed varte den 15-sekunder lange TV-reklamen videre gjennom folks IPAer frem til forbrukeren selv ba assistenten sin slutte (Anderson, 2017). Reklamestuntet til Burger King avslørte hvor lett det er å lure, eller kapre disse enhetene. Dette stuntet var nokså uskyldig i den forstand, men som Anderson (2017) hevder, viser denne reklamen hvor lett det kan være å gjøre ordentlig skade. Eksempelvis om en kriminell person klarer å aktivere en IPA, og for eksempel ber den låse opp døren (Anderson, 2017).

Informantene ble derfor spurt hva deres tanker var rundt nettopp risikoen for at uvedkommende kunne finne en måte å koble seg til deres IPA, og dermed få direkte tilgang til innsiden av hjemmet deres gjennom mikrofonen. Her er de fleste ubekymret, og de ser det som lite sannsynlig. Av 11 informanter, svarte to stykker av de var bekymret for hacking. To kvinnelig informanter hvor én er fra Norge og én er fra USA.

Informantene som ikke er bekymret for hacking begrunner dette først og fremst med at det er liten sannsynlighet for at nettopp dem skal bli utsatt for hacking, slik 24 år Mina forklarer:

> Man tenker jo liksom at ja det kan skje, men hva er sannsynligheten for at nettopp jeg skal bli utsatt for det. Man ufarliggjør det litt ved å tenke at sannsynligheten er så liten. Tanken har jo streifet meg, sånn at noen kan lytte på det jeg sier eller gjør ved å hacke hva som helst, men jeg tror bare jeg har blåst det vekk ved å bare.. jaja, det går greit. (Mina)

Mina er altså klar over at risikoen er der, men ufarliggjør det ved å tenke at sannsynligheten er liten. Også 26 år gamle Ole betrygger seg selv med samme argument:

> Det er ikke noe jeg er bekymret for, men jeg ser at det kan skje. Men jeg tenker sånn, det er så mange mennesker i verden, hvorfor vil man hacke seg inn på akkurat min. (Ole)

26 år gamle Josh begrunner sin ubekymrede holdning med at han ikke har noe spesielt spennende jobb, og ser det derfor som usannsynlig at noen skulle ville hacke nettopp han:

> I'm not concerned with like a targeted hack, just because I don't have a big job, there is no reason for anyone to target me. I'm more concerned with negligence leading to a big list of e-mail coming out and I just get bombarded with spam or something. (Josh)

Hans bekymring er derfor ikke fra andre mennesker, eller fra målrettet hacking, men heller menneskelig feil og forsømmelse, som kan i verste fall føre til utleveringen av hans e-post, som kan føre til spam-mail. 28 år gamle Michael er heller ikke bekymret for hacking, men sier at sannsynligheten er der, fordi det alltid er noen som blir hacket. Han forklarer det på følgende måte:

> Hacking is one of those things like, in its ignorance I guess, like it wouldn't happen to me. But again, thinking about it, it could definitely be a possibility and plausibility. When it comes to hacking, like it's got to be somebody, right? (Michael)

29 år gamle Sara og 24 år gamle Rachel derimot, er begge bekymret for hacking. For Rachel er frykten for hacking grunnen til at hun ikke ønsker en IPA med innebygget kamera:

> I think hacking is pretty spooky, and that is the reason why I won't get one of those with the camera. I mean, potentially someone watching me, in my house, you know, just no. (Rachel)

Rachel ønsker ikke å ha en IPA med innebygget kamera, nettopp fordi hun er redd for hackere som potensielt kunne fått tilgang til et kamera på innsiden av hjemmet hennes. For Sara var mulighet for hacking av IPA-mikrofonen en årsak til at hun valgt å koble den ut, og slutte å bruke den:

> Man er aldri 100% sikker når det gjelder hacking. Det er mange i verden som holder på med det der, og du kan gjøre det mot hvem som helst. Tanken på at noen skal lytte på det som skjer i leiligheten min er jo kjempeekkelt. Man mister kontrollen. Jeg ville ikke at noen skulle ha mulighet til å hacke den, så jeg ville ikke lenger ha den i. (Sara)

Hacking ser ikke ut til å være en generell bekymring for informantene, da de ser det som usannsynlig, eller at det er lite informasjon å få tak i gjennom deres IPA. For de som derimot frykter hacking, så har dette påvirket deres bruk av IPA. Rachel ønsker ikke å gå til innkjøp av en assistent med kamera, i frykten for at noen kan se på henne hjemme uten hennes samtykke eller kjennskap, og for Sara var frykten for hacking en påvirkende faktor til at hun valgte å frakoble sin IPA permanent.

4.3. Gratis IPA mot innpass i hjemmet

Av 11 informanter var det kun tre stykker som hadde gått til innkjøp av en assistent selv. Resten hadde fått sin i gave, eller fått den med på kjøpet i en kampanje. De sistnevnte er det interessant å se nærmere på: Hvordan har informantene opplevd å få tilsendt en IPA. Sander fikk sin første Google Home i gave fra arbeidsplassen sin. Så fikk han en spillkonsoll med integrert Google-assistent:

> Jeg kjøpte en sånn kampanje, og da fikk jeg med en spillkonsoll gratis. Jeg betalte vel 400 kroner for et spill, så fikk jeg i tillegg en Chromecast, denne spillkonsollen som koster over 1000 kroner til vanlig og har assistenten i seg, og noe mer på kjøpet. (Sander)

Til tross for at han som forbruker var storfornøyd med kampanjen, og sier han har brukt spillkonsollen mye i ettertid, stusser Sander likevel over hvorfor han får gratisprodukter som i utgangspunktet koster så mye, med på kjøpet av et langt rimeligere spill.

> Det er jo en kjempegod kampanje, men hvorfor får jeg denne gratis? Jeg som kunde er jo dritfornøyd, jeg elsker den jo. Men når det er en så positiv side så må det jo være en bakside også. Kanskje de vil at flere skal bli eksponert for assistenten, at de skal ha disse enhetene i så mange hus så mulig. (Sander)

Sander mistenker at leverandøren, i dette tilfellet Google, kjører kampanjer som nesten er for gode til å være sanne, for å få assistenten inn i så mange husstander som mulig. Det at han fikk en gratis spillkonsoll gjorde også at han valgte å abonnere på deres spilltjeneste:

> De har jo også med spilltjenesten en abonnementstjeneste. Og etter at jeg fikk denne konsollen så har jeg valgt å abonnere. Så til syvende og sist er det sikkert for å tjene penger. Men jeg er fornøyd. (Sander)

I dette tilfellet fikk Sander en konsoll på kjøpet, som er dyrere enn hans opprinnelige kjøp. Likevel resulterte det i at Sander aktivt tok i bruk konsollen, og i tillegg valgte han å abonnere på Googles spilltjeneste. Etter en stund vil dermed Google ha tjent inn pengene på konsollen, og de har fått assistenten plassert i enda en av Sander sine enheter. Også amerikanske Brian fikk sin IPA gratis gjennom en kampanje som virket nesten for god til å være sann:

> My Google Home was free. It was like, for some reason, if you had Spotify, they gave everyone a Google Home. Which is funny, because looking back at it, I was like *"what are they gaining?",* because they cost about a hundred bucks usually, and they gave them out for free if you had a ten dollar a monthly subscription. (Brian)

Brian abonnerte altså på musikktjenesten Spotify, og sier det koster omtrent 10 dollar (85 NOK, d.d) i måneden. Likevel fikk han med en enhet som koster over 100 dollar (850 NOK, d.d). Han mistenker at denne kampanjen blir gjennomført uten økonomiske tap for leverandør, takket være datainnsamlingen IPA gjør:

> I feel like the reason they gave them out was data collection. I mean, if anyone who pays for Spotify getting a hundred dollar-device, I mean, you have to make money somewhere. And I would assume it's because they collect a lot of data. (Brian)

Flere av informantene har altså fått en gratis IPA i en kampanje som de selv mener virker for god til å være sann. Andre sier de har fått den i gave. Som Sander og Brian sier, har de begge vært skeptiske til hvordan slike kampanjer kan være lønnsomt for leverandør, men uavhengig av årsak har begge valgt å ta den i bruk. I disse tilfellene har altså Google lykkes med å få innpass i flere hjem, og blitt en del av folks hverdag. Å bruke disse IPAene i flere dagligdagse situasjoner, som f.eks Sanders spillkonsoll vil naturligvis produsere enda mer råmateriale som igjen kan brukes for kommersiell utvinning (Zuboff, 2019), og det er de moderne, digitale plattformene som netthandel, kommunikasjon og smarte infrastruktursystemer som produserer enorme mengder detaljerte data om brukeren. Alt fra deres preferanser og mønster i adferd, til deres håp, tro og ønsker (Cinnamon, 2017). Derfor vil det trolig fra Googles side være en smart markedsstrategi å få plassert så mange IPAer i så mange hjem som mulig, noe som kanskje resulterer i kampanjene som Sander og Brian beskriver.

4.4. Oppsummering

Overvåking er noe alle informantene kan reflekterer rundt, og de har en samlet oppfatning av at overvåking er når noen eller noe forsøker å få tak i informasjon om deg. Flere trekker frem at det er et negativt ladet begrep, samtidig som enkelte informanter sier det kan ha en positiv effekt, dersom det er høyt trusselbilde. Informantene som har en positiv holdning til overvåking i enkelte situasjoner, er alle over 25 år. Dette kan ha en sammenheng med at informantene over 25 år kanskje husker terrorangrep som 9/11 bedre, hvor overvåking som sikkerhetstiltak ble diskutert i ettertid (Mathiesen, 2013). Frykten for overvåking ser ut til å være effektivt. Flere er engstelig for å bli overvåket i hjemmet, og oppfattet som kriminell, mens andre mener de ikke har noe å skjule, og dermed ikke bryr seg. I informantenes refleksjoner rundt IPA og overvåking, er det svært få som trekker frem kommersiell overvåking. Det ser derfor ut til at de færreste informantene forstår konseptet kommersiell overvåking. De anser i større grad overvåking som noe skjer i forbindelse med terror og kriminalsaker. I neste kapittel vil jeg analysere hvordan informantene reflekterer rundt eget personvern.

5. Personvern

I analysens andre dimensjon vil jeg se nærmere på informantens forhold til eget personvern, og hvor viktig de synes det er å verne om personlig informasjon. I dagens digitaliserte samfunn, med sosioteknologiske systemer som kontrollerer og håndterer informasjonsstrømmen, kan det være vanskelig å definere personvern, og dets verdi. Vi beskytter tingene og kontoene våre med passord, og ønsker kanskje ikke å legge igjen personnummer, adresse, telefonnummer eller andre identifikatorer overalt. Men hvordan forholder vi oss til dette fenomenet som er så vanskelig å definere? James H. Moor (1997) foreslår at personvern bør ses på som noe todelt. På den ene siden, noe som er veldig viktig og som man bør strekke seg langt for beskytte. På den andre siden noe som kan defineres av personlig preferanser, kulturelle påvirkninger, og noe det generelt er vanskelig å fastslå viktigheten av. Jeg vil nå se nærmere på informantenes oppfatning av personvernsbegrepet, og hvor viktig det er for hver enkelt informant. Jeg ønsker å se om det kommer frem tydelig kulturelle forskjeller, slik Moor (1997) foreslår, eller om personvernsbegrepet blir oppfattet likt av unge mennesker i 20-årene, uavhengig av kultur, kjønn eller andre faktorer. I dette kapittelet vil kulturelle forskjeller få et naturlig fokus, da Norge, med bakgrunn i EØS-avtalen, har tatt GDPR (EUs personvernforordning) inn i norsk lovverk. Denne personvernforordningen presiserer adgangen til å gjennomføre enkelte behandlinger av personopplysninger (Regjeringen, 2019). Selskaper må følge strenge retningslinjer om hvordan de kan samle inn og bruke opplysninger, og enkeltpersoner har en rekke rettigheter til innsyn, retting og sletting av sine personlig opplysninger (Datilsynet, 2018). Praktisering av personvernforordningen er trolig noe enkeltpersoner merker lite til i hverdagen. Derfor har jeg valgt å ikke fokusere for mye på dette relativt nyetablerte reglementet, men heller se hvordan kulturelle forskjeller spiller inn, hvor ett land (Norge) har strenge retningslinjer, og det andre (USA) har ikke.

5.1. Holdninger til personvernbegrepet

Informantene ble aller først bedt om å selv definere begrepet. Norske Sara legger vekt på kontroll over egne opplysninger:

> Personvern ser jeg på som at du har kontroll over opplysningene dine. At du vet hva som blir innhentet om deg. Personvern er jo for å unngå misbruk av dine opplysninger. (Sara)

For Sara er kontroll over egne opplysninger viktig for å unngå misbruk av hennes opplysninger. Amerikanske Michael derimot, vektlegger *frihet* i måten han beskriver personvern:

> Privacy is having the ability to have discussions, interactions and alone moments, without the threat of someone seeing, hearing or interacting with those alone moments I guess. In regards to the speakers I don't know if there are any privacy. You know, it's not supposed to listen, but, who knows how true that is. (Michael)

For Michael er altså ikke misbruk av personopplysninger den største faktoren i hvordan han definerer personvern. Han vektlegger i stedet muligheten til å si hva man vil i eget hjem, uten å risikere at uvedkommende lytter til private samtaler. Også amerikanske Rachel definerer personvern utfra frihet til å si hva man vil i private sfærer:

> Well, privacy is like, you feel like in your own home you can say whatever you want and not feel like anyone is watching you. And that is what I feel like privacy should be. (Rachel)

For Norske Sara er altså personvern et middel til å oppnå sikkerhet, og dermed unngå misbruk av personopplysninger. For amerikanske Michael og Rachel er personvern noe de anser som en viktig del av friheten til å ytre seg som man vil, uten å risikere at andre får tilgang til deres private samtaler. Informantene fra ulik kultur definerer altså personvernet på ulike måte, men i begge tilfeller blir personvernet ansett som et middel i å oppnå et mål. Personvern som et middel til å oppnå et mål er hvordan Moor (1997) definerer personvernets instrumentelle verdi. I tillegg vektlegger informantene enten sikkerhet eller frihet, som begge kan anses å være kjerneverdier i et samfunn. Moor (1997) argumenterer for at personvern defineres av personlig preferanser og kulturell påvirkning, noe som ser ut til å stemme blant studiens informanter.

5.2. Personvern som et middel til å oppnå frihet og sikkerhet

Verdi er noe som måler kvaliteten ved noe, og det er noe som kan tilegnes alle ting, som personer, objekter, handlinger og tilstander (Sagdahl, 2019). Det skilles gjerne mellom to typer verdi, nemlig *egenverdi*, og *instrumentell* verdi. Ting som har egenverdi er verdifullt som det er, mens instrumentell verdi har verdi som et middel til å realisere noe med egenverdi (Sagdahl, 2019). De fleste ville nok sagt seg enig i at personvern er viktig for å beskytte personlig informasjon. Vi beskytter tingene og kontoene våre med passord, og deler gjerne

ikke personnummer, telefonnummer og adressen vår helt ukritisk. Vi verner om informasjonen vår, slik at personer med uærlig hensikter ikke skal få tak i det, på samme måte som at Sara ønsker kontroll på egne opplysninger, slik at det ikke skal bli misbrukt. Dette er slik Moor argumenterer for at personvern har instrumentell verdi (Moor, 1997, s. 29). Egenverdi derimot, er litt mer komplisert. Debora Johnson (1994) påstår at personvern er en essensiell del av menneskers selvstyrerett. Og hvis selvstyrerett har egenverdi, og personvern er en vesentlig del av selvstyreretten, slik Johnson (1994) mener, så kan man argumentere for at personvern også har indirekte egenverdi, foreslår James H. Moor (1997, s. 28). Jeg vil nå se nærmere på hvilken verdi personvernet har for informantene. De ble derfor spurt hvor viktig personvern er for dem. Norske Sander glemmer ofte å tenke over personvern når han implementerer ny teknologi i sin hverdag:

> Jeg tror det er blitt så enkelt å bruke nye ting på en måte, så den personvernsbiten tenker man liksom ikke mye over. Også føler jeg at du må jo bare godta personverngreiene når du skal bruke nye ting. (Sander)

For Sander er det altså enklest å bare godta personvernerklæringen når han tar i bruk nye ting, noe han ikke er alene om. Ingen av de 11 informantene har lest personvernerklæringen til sin IPA. Avtaler mellom forbruker og datainnsamler har tidligere fått kritikk for å være utnyttende, fordi forbrukeren ofte ikke har tilstrekkelig kunnskap om omfanget av datainnsamlingen (Cinnamon, 2017). Avtalen er ofte urettferdig, men også unngåelig, og noe forbrukeren ikke kan forhandle om. Deres eneste alternativ blir da å være offline (Peacock, 2014, s. 8). Norske Ole tar det veldig med ro når det gjelder eget personvern, og sier han ikke tenker noe særlig over det:

> Jeg er veldig slækk når det gjelder personvern. Jeg legger kanskje ikke personnummer igjen overalt, men personopplysninger om meg synes jeg ikke er så farlig å dele. (Ole)

Ole ser det altså ikke som en potensiell trussel å legge igjen, eller la andre få tilgang til hans informasjon. Han setter likevel en grense ved personnummeret sitt. Ole ble spurt om han alltid godtar informasjonskapsler, eller personvernserklæringer på nye enheter eller nettsider han besøker, noe han bekreftet at han gjør. Ole og Sander er to eksempler på informanter som ikke nødvendigvis ser den instrumentelle verdien av personvern. Informanter som Sara, Rachel og Josh er derimot på motsatt side av skalaen og bruker personvern som et aktivt middel for å

oppnå sikkerhet. Norske Sara, som koblet ut sin IPA, sier hun ofte sjekker opp en tjenestes legitimitet før hun legger igjen personopplysninger:

> Jeg synes personvern er viktig og vil si at jeg er ganske nøye på det. Jeg bruker for eksempel TrustPilot mye for å sjekke ut hvilke tilbakemeldinger selskaper og nettsider har fått. Og jeg bruker de tingene jeg vet om for å bekrefte at ting er greit. Jeg liker ikke å legge igjen informasjon uten å ha sjekket at ting er greit først. (Sara)

Hun benytter seg altså av tilleggstjenester som TrustPilot for å undersøke et selskaps legitimitet, før hun legger igjen informasjon. Dette gir henne muligheten til å se andre kunders erfaringer, og hun får en generell vurdering av selskapet. Også amerikanske Rachel tar liknende grep som Sara, og gjør sine forhåndsundersøkelser for å være sikker på at hennes informasjon ikke blir misbrukt av useriøse aktører:

> When I'm signing up for something new and its asking for a lot of information I definitely do more of a background check on what this company is, and if they are safe and what not. Because I feel like my information is definitely private, and I want keep it as private as I can. (Rachel)

Amerikanske Josh går enda lenger enn Sara og Rachel for å beskytte sitt personvern. Han mener alt på nett kan logges, og dermed ikke lenger er like privat. Han beskriver tiltakene han har gjort for å sikre sitt personvern:

> Privacy is important to me, particularly for devices. If something is too cheap to believe, there is a pretty good chance that the server is set up in China somewhere, and they're doing whatever with your information. (Josh)

Josh er bevisst på hvor produktene han installerer i hjemmet sitt kommer fra. Han ønsker å ha produkter koblet til servere i USA, for økt følelse av kontroll. Josh hadde tidligere lysbrytere fra Kina, men forteller at han var usikker på hva som skjedde med hans data:

> Previously I had a bunch of Chinese light switches, and they were like 12 bucks a switch, really cheap. And I had that until I started thinking about where they were going, and who was talking to them, because obviously it's not locally controlled. So when I would turn on the light from my phone, it would bounce to china, and bounce to google and then turn on my lights. And I did not like that. (Josh)

Josh var ikke komfortabel med at informasjonen fra hjemmet hans ble sendt til en server i Kina, og bestemte seg for å gjøre hjemmet hans så offline som mulig, med en egen server:

> All the smart home stuff that I have that is not through google is all flashed with offline software that I run from a home assistant server over here. And it's all on its own VLAN. I mean it is as offline as I can make it. And then google is the front end, because I trust google with my stuff back and forth. (Josh)

Josh stoler altså på leverandøren Google, men ønsker ikke å dele sin informasjon med servere i for eksempel Kina. Han forklarer dette med at han ikke vet hva som skjer med informasjonen hans når han ikke lenger har kontroll på hvor det havner, og har derfor valgt å koble sine produkter som ikke er levert av Google, på et offline VLAN, slik at informasjonen ikke blir sendt videre til andre aktører.

Det viser seg at informantene er svært delt når det kommer til deres syn på personvernets instrumentelle verdi, og alle ser det nødvendigvis ikke som et middel til å oppnå sikkerhet. Ole og Sander er mindre kritiske til hvor og hvem de deler informasjonen sin med, og Ole mener at det er noe man må godta om man skal ta i bruk ny teknologi, noe Cinnamon (2017) også argumenterer for, da hun mener avtalene skapt innen overvåkingskapitalisme er uunngåelig for forbrukere, og deres eneste mulighet er å være offline. På den andre siden er personvernets instrumentelle verdi svært viktig for informanter som Sara, Rachel og Josh, som alle tar forskjellig grep for å sørge for at deres informasjon ikke havner hos et selskap de ikke anser som seriøst og legitimt. Josh er den informanten som har gått lengst i å beskytte sitt personvern, og sørger for at utenlandske selskaper ikke får tilgang til informasjon produktene i huset hans kan avsløre, og har opprettet en offline programvare på en egen server, og et privat VLAN. Det ser ut til å være lite kulturelle forskjeller, men den gruppen som kan tolkes å være den som er minst opptatt av personvernets instrumentelle verdi, er unge norske menn, som Sander og Ole.

5.3. Er personvernet viktig for selvstyreretten?

Informantene har ulike oppfatninger av personvernets verdi som et middel til å oppnå trygghet, men hva med personvernet i seg selv? Moors (1997) andre måte å definere personvernets verdi på, er dets egenverdi. Debora Johnson (1994) påstår at personvern er en essensiell del av menneskers selvstyrerett. Og hvis selvstyrerett har egenverdi, og personvern er en vesentlig del av selvstyreretten, så kan man argumentere for at personvern også har

indirekte egenverdi, foreslår James H. Moor (1997, s. 28). Han bruker eksempelet om datakyndige «Tom» for å utfordre idéen om at personvern har egenverdi. «Tom» er en person som bruker all sin tid på å få vite så mye som mulig om deg, uten at du er klar over det (Moor, 1997, s. 29). Som Moor argumenterer, ville de fleste tenkt at slik overvåking ville vært ubehagelig, selv om informasjonen ikke ble delt videre, eller brukt til å skade deg. Du ville med andre ord hatt full selvstyrerett, men ikke lenger noe privatliv eller beskyttelse mot overvåkingen fra «Tom» (Moor, 1997, s. 29). Han utfordrer med dette Johnsons (1994) påstand om at personvern er essensielt for menneskers selvstyrerett. Enkelte av informantene trekker frem nettopp det å bli overvåket av et annet menneske, og mener det er stor forskjell på andre mennesker som får tilgang til deres opplysninger, slik som eksempelet med «Tom», og store selskaper som Google. Norske Thomas beskriver forskjellen på følgende måte:

> Jeg synes det hadde vært mye verre hvis jeg hadde hatt en person utenfor vinduet mitt som lyttet til det jeg sa, i forhold til Alexa. Med et menneske er det mye mer fysisk med en gang. (Thomas)

Mange ville trolig sagt seg enig med Thomas. Men si man bytter ut «Tom» med Google eller Amazon. Er da dette eksempelet til Moor egentlig så langt unna hverdagen til IPA-brukere? Assistenten har en alltid-lyttende mikrofon, og logger alt av samtaler og interaksjoner mellom forbruker og IPA. Informasjonen som blir samlet inn, blir ikke brukt til å gjøre skade, men som Zuboff påstår, blir denne informasjonen brukt til å forutse, og til og med forsøke å endre oppførselen til forbrukeren. Hun går så langt som å kalle det et angrep på menneskets frie vilje (Zuboff, 2019). Det kan derfor argumenteres for at Google legger opp til at selskaper kan påvirke deres forbrukere. Naturligvis vil resultatet av denne påvirkningen variere. Mina tror at store selskaper med mye informasjon om individer, kan indirekte påvirke mennesker i sin favør:

> Man lever jo egentlig i en verden hvor man føler man er sykt anonym, privat, og ingen kjenner deg ordentlig. Men så sitter store selskaper på informasjon som gjør at enhver kan påvirke deg i sitt favør. Annonsering av politiske innlegg eller religiøse syn kan jo reklameres for hos en person hvor det er større sannsynlighet for at de vil gjøre noe i deres favør. Om det gir mening. (Mina)

Moor (1997) foreslår at personvern har en indirekte egenverdi i den forstand at selvstyrerett har egenverdi, og personvernet er en del av menneskers selvstyrerett. Dette er også Mina inne på, da hun mener at til tross for at man føler seg anonym og veldig privat i dagens samfunn, så

sitter store selskaper på så mye av din informasjon at de kan tilpasse dine annonser, og resultatet kan være at du blir påvirket i deres favør. Minas refleksjoner viser en direkte påvirkning av selvstyreretten, og dermed kan det argumenteres for at personvernet har indirekte egenverdi.

5.4. Samfunnets rammeverk

Informantene definerer personvernet i seg selv, og hvor viktig det er for dem på svært forskjellig måter. Mens informanter som Sander og Ole ikke nødvendigvis ser den instrumentelle verdien av personvern, betyr personvern sikkerhet for norske Sara. For amerikanerne Rachel og Michael, betyr personvern frihet. Norske Mina beskriver en ubevisst påvirkning, som Moor (1997) foreslår er en innvirkning på menneskets frie vilje. Både sikkerhet, frihet og selvstyrerett er hva Moor (1997) beskriver som et samfunns *kjerneverdier*, og noe som finnes i ethvert samfunn i varierende grad utfra ulike kulturelle forskjeller. Hvis man da bruker kjerneverdiene beskrevet ovenfor som et rammeverk, så kan man slik Moor (1997) foreslår, si at personvern har både instrumentell verdi, da det er en støtte for kjerneverdiene, slik Sara søker sikkerhet, og Michael og Rachel søker frihet. I tillegg kan personvernet sies å ha egenverdi, da det er en måte å utrykke sikkerhet på (Moor, 1997, s. 30). Jeg mener sikkerhet, slik Moor (1997) foreslår, ikke bare er for å hindre uvedkommende fra å få tilgang til din informasjon, men også for å beskytte hele selvstyreretten, og beskytte seg fra påvirkning fra overvåkingskapitalister som innhenter og behandler mengder med data fra sine forbrukere.

Det kan altså sies å være kjerneverdiene i samfunnet som påvirker informantenes syn på personvern. Det er lite kulturelle forskjeller som skiller de norske og amerikanske informantenes syn på viktigheten av personvern. Samtidig kan de ulike kjerneverdiene informantene vektlegger skyldes kulturelle forskjeller. Mens flere av de amerikanske informantene definerer personvern som *frihet,* definerer norske Sara det som kontroll, eller en sikkerhet rundt at ikke uvedkommende ikke får tilgang til hennes informasjon. I tillegg er det gruppen unge, norske menn som skiller seg ut som gruppen som ser minst verdi i personvernet.

5.5. Kontekstuell integritet

Personvern er viktig for de fleste av informantene, og til tross for at de definerer personvern noe ulikt, er definisjonene basert på samfunnets kjerneverdier, og personvernets instrumentelle verdi. Men hvordan forhandler de om personvernet sitt i praksis? Jeg vil nå se nærmere på informantenes holdning til personvern i bruken av IPA-systemer. For å gjøre dette, vil jeg benytte meg Helen Nissenbaums teori om kontekstuell integritet. Teorien baseres på fire nøkkelprinsipper som må overholdes for at mennesker ikke skal føle at det har vært et brudd på deres personvern. De fire prinsippene *normer, aktører, informasjonskarakter og overføringsprinsipper* (Nissenbaum, 2010) For at den kontekstuelle integriteten skal ivaretas, er det viktig at våre forventninger til strømmen av personlige opplysninger blir møtt og ivaretatt (Nissenbaum, 2010, s. 233).

5.5.1. Tillitt til aktøren

Informantene fikk spørsmål om de stoler på Google og Amazon (avhengig av hvilken IPA de eier) til å ivareta deres personvern. Med unntak av informanten som har valgt å koble ut sin IPA, har informantene stort sett tillitt til selskaper som Google og Amazon. Hos flere legges det vekt på at et stort sikkerhetsbrudd hos en av aktørene ville vært langt mer skadelig for aktøren selv, i forhold til forbrukeren. Dermed slår de seg til ro med at Google og Amazon beskytter deres personlig informasjon fra uønskede tredjeparter. Amerikanske Taylor føler en trygghet når hun deler sin informasjon med store selskaper. Hun føler seg trygg på at selskapet ville fått konsekvenser dersom de misbruker tillitten de blir vist av forbrukerne:

> Yeah, I trust them. I feel like they're a big enough company that like, if there was a data breach or something, there would be consequences. (Taylor)

Til tross for at de fleste informantene svarer ja på spørsmålet om de stoler på aktøren, er det flere som har en viss skepsis, slik norske Eirik forklarer:

> Ja, jeg stoler på dem, men det er litt sånn... det er nok litt shady. Informasjon blir nok ikke misbrukt, og jeg tror ikke andre får tilgang. Vi gir dem jo tillatelse til diverse når man setter opp en google home, men jeg tror ikke det blir misbrukt til reklame eller til noe som ikke er greit da, sånn rent etisk. For da vil jeg igjen tro at det vil skade googles rykte og forretningsmodell såpass mye at det ikke er verdt det rett og slett da. (Eirik)

Det Eirik sier her, kan tolkes som at han mener det kun er Google som får tilgang til hans informasjon, og at forbrukerdataen som IPAen produserer, ikke blir brukt til målrettet reklame. Teoretikere som Zuboff og Thornhill mener derimot at forbrukerdata blir brukt i kommersielle sammenhenger. I tillegg hevder de at det blir laget produkter med den hensikt å suge til seg hver eneste bit informasjon på det digitale kartet, hvor enheter som IPAer, nettshopping og smart-hjem bidrar til å produsere denne type data (Thornhill, 2019). Zuboff hevder disse menneskelige erfaringene er selve råmaterialet som blir analysert til forutsigbar oppførsel, som dermed kan forutse forbrukeren fremtidig trekk, og finne ut hvordan disse kan påvirkes (Zuboff, 2019). Sara, som har frakoblet sin IPA, stoler ikke på aktøren Amazon, og forklarer følgende:

> Nei, jeg stoler ikke på dem. Jeg tror når det kommer til penger, og siden det er så mange som har kjøpt Amazon Echo, så blir man litt sånn umenneskeliggjort. Kanskje at de anser deg som bare et produkt som de kan selge videre, og det er jo ikke greit. Men når det gjelder penger, så gjør jo folk alt for å få tilgang til din informasjon. De bryr seg ikke så veldig om deg som enkeltperson da. (Sara)

Samtidig som andre informanter stoler på aktøren *fordi* det er et stort selskap, er dette grunnen til at Sara ikke stoler på aktøren. Hun mener det hele handler om penger, og at man som forbruker kun blir ansett som et produkt selskapet kan selge videre. Slik jeg tolker det, er Sara den informanten som reflekterer noenlunde likt som teoretikere som Zuboff (2019) og Thornhill (2019). Idéen om at man som forbruker blir ansett som en kilde til menneskelig råmateriale selskapene er ute etter å fange opp og analysere for fremtidig salg. Med unntak av Sara, stoler samtlige av informantene på aktøren til å beskytte deres personlige opplysninger. Den største grunnen til denne tillitten er oppfatningen om at personvernbrudd vil skade de store selskapene mer enn forbrukeren dersom tillitten ble misbrukt.

5.5.2. «Hæ, lagres det?»

Helen Nissenbaum (2010) skriver at normer kan sees på som oppførsel vi anser å være akseptabel. Normene kan definere forholdet mellom aktørene, og dermed være avgjørende for maktforholdet som definerer flere sosiale kontekster (2010, s. 143). I dette tilfellet gjelder det forbruker og leverandør. De fleste informantene stoler altså på leverandøren, og de føler seg trygge på at informasjonen deres ikke havner på avveie, så lenge fallhøyden er større for leverandøren enn dem selv. Så hvordan stiller de seg til bruken av deres personlige samtaler med assistenten? Informantene ble informert om at alle deres samtaler med assistenten blir

lagret permanent, med mindre man selv har gått inn for å endre eller skru av denne funksjonen. Av 11 informanter var det kun to stykker som var klar over at lagring av samtaler var en funksjon, og at forbrukeren selv kan lytte til opptakene. Ole ble overrasket og skremt av at hans samtaler ikke ble slettet umiddelbart:

> Hæ, er det sant? Det var jeg ikke klar over engang, hvor lett finner jeg det? Det er jo jævlig skummelt da. Jeg visste ikke at det gikk an, men jeg kommer til å gå inn for å høre på det nå. (Ole)

Informantene som ikke var klar over denne funksjonen så det som ubehagelig, skummelt og ekkelt at det ikke var noe som tydelig blir presisert av Google. Rachel føler hun aldri har godkjent at samtaler mellom henne selv og assistenten lagres:

> Noo, that is so creepy, oh my god. I didn't know that happened. I feel like I never have agreed to anything like that, but I'm sure if go back and read the fine print I feel like it's there somewhere, but they make it so easy to set up and stuff, it's just like "oh here, it's fine", but yeah, that is definitely a little worrisome. So creepy, I didn't know they did that, actually. (Rachel)

Rachel opplever altså denne funksjonen som ubehagelig. Til tross for at hun ikke har lest personvernserklæringen, kan det tolkes som at Rachel har antatt at sletting av lydopptak er normen, altså akseptabel oppførsel. Hun reagerer derfor på en negativ måte når hun ikke opplever at dette er gjort. Josh, en av informantene som faktisk var klar over denne funksjonen, mener det kan ha sine fordeler at interaksjoner blir lagret, og har valgt å ikke skru av denne standard personverninnstillingen som godkjenner lagring av interaksjoner permanent:

> I do have that on. Just in case something, like if it were to start talking to me in the middle of the night, I can go back and see what it heard. Maybe I had said something in my sleep, I have no idea. So it would be handy to go back and find that, and you know, It's not like they´re not storing it anyways, so I would like to get access to whatever it is. (Josh)

For Josh er det altså viktigere å ha tilgang til samme informasjon som leverandøren har tilgang til. Ettersom han tror Google ville lagret samtaler uansett, så mener han det er det en fordel som forbruker å kunne få tilgang til disse opptakene. Når informantene ble spurt om hvorfor de tror det er en funksjon at alle samtaler blir lagret permanent, er det stor variasjon

blant informantene. Mina følte seg mer overvåket når hun ble gjort oppmerksom på funksjonen:

> I utgangspunktet så er min umiddelbare tanke at de lagrer det for å kartlegge meg som person. Men jeg synes likevel det er likevel det er merkelig at de skal bli lagret over så lang tid, at det ikke er sånn at de blir slettet etter en stund. Jeg vet ikke hensikten annet enn det, men det føles litt utrygt ut. Man føler jo at man blir overvåket. (Mina)

I tillegg til Mina, føler også Sara seg overvåket etter å ha blitt gjort oppmerksom på denne funksjonen. Hun tror det er en funksjon som blir brukt til målrettet markedsføring, slik at leverandører tjener penger på interaksjonene med sine forbruker. Hos de andre norske informantene er det enten markedsføring eller forbedring av brukervennlighet som blir nevnt. Amerikanske Josh mener det er en funksjon fordi man som forbruker bør ha tilgang til sin egen stemme:

> Well, it's your voice. And it is something you are interacting with regularly. And frankly, you know, if they didn't have the option, I would not be bothered. But because they do have it, I will listen in. Because at some point some will say "my Google home started talking to me last night, I want to hear what it heard". (Josh)

Josh tror ikke han hadde brydd seg om Google ikke hadde gitt forbrukeren muligheten til å høre gjennom interaksjoner, men velger å ha funksjonen skrudd på i tilfelle assistenten snakker av seg selv, slik at han kan ha kontroll over hva IPAen har reagert på. De norske nevner altså enten markedsføring eller forbedring av brukervennlighet som hvorfor de tror det er en funksjon. Markedsføring eller forbedret brukervennlighet blir derimot ikke nevnt av noen av de amerikanske informantene. Av informantene fra USA sier tre av fem at de ikke kan komme på noen grunn for at det skal være en funksjon, én mener det er for leverandørens fordel, men usikkert hvordan, og siste er som Josh sier, fordi det er din stemme som blir tatt opp.

5.5.3. Menneskelig avlytting

I tillegg til samtaler som blir lagret, blir også vilkårlige samtaler fra både Google og Amazon lyttet til av menneskelig ansatte i selskapene (Day & Drozdiak, 2019). Da informantene ble informert om at deres lydopptak kan potensielt bli lyttet til av ansatte, ble de fleste overrasket. Her var det kun amerikanske Josh som var klar over dette, og han mener dette ikke er noe folk flest vil få vite om, med mindre de følger med på ukentlig oppdateringer:

> About six months ago it was discovered that some of the recordings were going through actual human listening, for better speech analysis. Unless you're plugged in and get like weekly news update, you are not going to know about that. (Josh)

Josh tror midlertidig ikke at det er den menneskelig avlyttingen i seg selv som nødvendigvis er det store problemet. Han mener problemet er at det er såpass skjult fra forbrukeren:

> Is the human listening a problem in and on itself? Depends on who you ask. But if their goal was to improve voice recognition, which everybody complains about, then they are in the rights to do that. But they should have been more forthright and notifying users, like *"hey, btw, some of your recordings can go to people, you can opt out of it".* So that needs to be the big thing. (Josh)

Han mener selskapet bør ha rett til å gjøre de forbedringene som trengs for å optimalisere produktet sitt. Likevel mener han det bør bli tydeliggjort fra leverandør sin side, og samtidig gi forbrukeren en mulighet til å reservere seg fra menneskelig avlytting. I tillegg mener han det bør være lettere å forstå hva man tillater når man tar en IPA inn i hjemmet sitt, og at personvernerklæringer bør skrives på en enkel og forståelig måte, fremfor juridisk tale:

> When you first buy a smart speaker, all the stuff you have to opt into and they can't hide it behind too much legal speech, it needs to be for people to understand what they're signing up for. Cause you can have a perfectly private home, if you didn't bring in smart speakers, and if you didn't have security cameras, it would be easy to live without it, and then you have your privacy at home. (Josh)

Resterende informanter stiller seg kritiske til at selskapene ikke er tydelig nok på at de tar opp lyd og benytter seg av menneskelig avlytting i forbedring av brukeropplevelsen. Michael mener de bør gjøre forbrukeren oppmerksom på at deres samtale kan blir lyttet til av et annet menneske:

> I did not know that, and that slightly bothers me. I definitely think they should be a little more honest and upfront, just have a little note on the app, with like a push notification the next time you´re using the app, that like random interactions are being reviewed by an in-person team. And maybe some justifications as to why they are doing it. But I don't understand the *why* behind the method. (Michael)

Brian opplever det at samtaler med IPAen kan gå gjennom menneskelig avlytting som et personvernbrudd.

> I would say that's definitely a breach of privacy, and probably something they're shielded against, but human listening would bother me. It probably wouldn't bother me enough to like, fight it, but the principle of it is just messed up. It just feels wrong. (Brian)

Ifølge Helen Nissenbaum (2010), er det først når det oppleves et brudd i en av de kontekstuelle byggesteinene at det kan sies å være brudd på personvernet. For informantene i dette tilfellet blir majoriteten av informanter altså overrasket til hvordan Google eller Amazon bruker og håndterer deres personlig data, opplever det som ubehagelig eller kritikkverdig at det ikke blir tilstrekkelig opplyst til forbrukerne. Brian opplever menneskelig avlytting som et brudd på personvernet. Informantene ser altså ut til å være komfortable med bruken av IPA, så lenge deres forventninger overholdes, noe informantene ikke opplever har blitt gjort i disse to eksemplene beskrevet ovenfor. Det er altså ikke informasjonen de deler med assistenten de anser som hemmelig, men de føler informasjonen deres har blitt delt med feil mennesker, uten deres tillatelse. Et slikt scenario beskriver Nissenbaum som en gjennomgående årsak til konflikt i personvernsaker (Nissenbaum, 2010, s. 142).

5.5.4. Informasjonskarakter

Informasjonskarakteren er avgjørende for hvorvidt informasjonen er passende eller upassende i gitte situasjoner, ifølge Nissenbaum (2010). Det er vanskelig å presentere et klart skille mellom passende og upassende informasjonskarakter, fordi kontekst, normer og roller varierer i ulike situasjoner (Nissenbaum, 2010). For å kunne se nærmere på den siste variabelen i kontekstuell integritet, skal jeg nå analysere informantenes holdninger til informasjon assistenten kan plukke opp. Informantene ble derfor spurt hva de anser som sensitiv data, utfra informasjon teknologiske enheter i hjemmet evner å samle inn. De ble også spurt om de noen gang har skrudd av mikrofonen til sin IPA i enkelte tilfeller. Alle informantene sier deres IPA er eller var plassert sentralt i hjemmet, og de kunne snakke til den fra de fleste rom i hjemmet sitt. Vanligvis stue, soverom og kjøkken. Informantenes IPA har dermed stor hørevidde, og kan plukke opp ord og samtaler fra flere rom. Thomas mener han aldri sier noe farlig rundt Alexa, og har derfor aldri skrudd av mikrofonen:

> Ting jeg sier rundt Alexa er ikke noe farlig informasjon. Det er ikke noe kriminelt eller sensitivt som jeg ikke skal si videre. (Thomas)

Taylor sier hun stort sett bruker Alexa til ting som ikke gjelder sensitiv informasjon, men passer på å ikke si sitt social security number rundt sin IPA:

> I use Alexa for nothing important. Like my grocery list, or something to add to my cart. But I don't say stuff like my social security number around her. (Taylor)

Tidligere studier viser at taleopptak og video fra innsiden av hjemmet er de datatypene folk anser som mest sensitive (Malkin, 2019). Samme resultat vises også i denne studien, da over halvparten av informantene sier at de anser taleopptak og private videoopptak som den mest sensitive datatypen. På tredjeplass kommer bilder. Sist kommer tekst, kortinformasjon og personnummer. Resultatene er presentert i tabellen nedenfor:

Datatype informantene anser som sensitiv informasjon	**Antall stemmer**
Taleopptak	6
Video fra innsiden av hjemme	6
Bilder	4
Tekst	2
Kortinformasjon	2
Personnummer/ Social Security Number	2

(Informantene kunne nevne mer enn én variabel)

Sara opplevde det som ubehagelig at mikrofonen alltid sto på. Hun sammenliknet det med å ha en uvedkommen i rommet til enhver tid:

> Jeg tenkte mye at jeg syntes det var ekkelt at den sto på hele tiden. Jeg følte litt at det var en uvedkommen i rommet, som hørte på, og som man måtte være litt forsiktig hva man sa foran, fordi det var en mulighet at den tok opp lyd. (Sara)

Med unntak av Sara har ingen av informantene skrudd av, eller kan huske at de har skrudd av IPAens mikrofon midlertidig. Dette til tross for at over halvparten anser taleopptak som sensitiv data, i tillegg til at flere har opplevd eller mistenkt at IPAen lytter til samtaler uten at triggerordet er sagt. Det at ingen informanter har skrudd av, eller kan huske å skrudd av

mikrofonen midlertidig, har trolig en sammenheng med at alle informantene, med unntak av Sara, har tillitt til IPA-leverandøren. Dermed anser de det som lite sannsynlig at deres sensitive opplysninger ville havnet på avveie, dersom IPAen hadde lagret informasjon av sensitiv karakter.

5.5.5. Overføringsprinsipper

Jeg vil nå se nærmere på overføringsprinsippet til Helen Nissenbaum (2010) i IPAens kontekst. Overføringsprinsipper setter en begrensing på informasjonsdeling fra en part til en en annen. I noen tilfeller er det informasjonens natur som ligger til grunn for dette prinsippet, i andre tilfeller kan det være rollebestemmelser eller andre variabler. Et eksempel på et slikt prinsipp kan være at en part som har mottatt informasjon, ikke får lov til å dele det videre (Nissenbaum, 2010).

Overføringsprinsippet vil i denne studien være mellom forbruker og leverandør, og hvilken informasjon som er akseptabelt å dele videre. Informantene fikk derfor spørsmål om hvem de synes skal ha tilgang til deres informasjon, og hvorvidt de stiller seg positive til at leverandøren kan dele deres informasjon med en tredjepart. Ole er av den oppfatning av det kun er han og Google som har tilgang til informasjon som IPAen samler inn:

> Jeg tenker at det er bare meg og google som kjenner til hva jeg sier til assistenten, og jeg synes ingen andre skal få den informasjonen. Hvis de skulle delt informasjonen da, så måtte det vært veldig tydelig sånn «vil du at en tredjepart skal motta dette?» (Ole)

Mina føler seg komfortabel med at informasjon som ikke sier noe om henne som person blir delt, men setter et tydelig skille mellom hva som er greit og hva som ikke er greit:

> Det kommer an på hva slags informasjon det er. Om et selskap får vite at «okei, her er det en jente i midten av 20-årene som liker sminke », så gjør ikke det meg noe. Men om det er informasjon utover det, sånn at jeg er i et forhold, er student, jobber deltid, sånn utover hva selskapet egentlig har bruk for, synes jeg blir unødvendig. Men nå vet ikke jeg hva som blir delt og ikke, det er jo det som er skummelt. (Mina)

For Mina går grensen på personlige opplysninger som kan avsløre mye om hvem hun er som person. Dette vil hun holde for seg selv, mens deling av generelle opplysninger og interessert stiller hun seg mer positiv til.

5.6. Oppsummering

Unge norske menn skiller seg ut fra øvrige informanter som mindre kritiske til hvor og hvem de deler informasjonen sin med. Norske Ole har satt en grense ved personnummeret sitt, men ellers bekymrer han seg lite om hvem som kan få tak i hans personopplysninger. Flere av de amerikanske informantene derimot tar aktive grep for å verne om sitt personvern. Eksempelvis Josh, som bevisst handler fra USA-baserte selskaper. I tillegg har han gjort hjemmet sitt så offline som mulig, og ønsker god kontroll på hvor informasjonen hans havner. Amerikanske Rachel og norske Sara undersøker selskaper før de legger igjen informasjon. Dette gjør de for å være sikre på at det er seriøse aktører.

De fleste sier personvern er viktig for dem, men likevel har ingen lest personvernerklæringen, og de er ikke klar over hvordan deres opplysninger blir håndtert i praksis. Informantene ble derfor overrasket over at menneskelig ansatte kan lytte til deres opptak, og at deres interaksjoner med assistenten blir lagret permanent, med mindre funksjonen blir skrudd av. Det er kun tre informanter som trekker frem spesifikke grep de tar for å beskytte personlig informasjon. Tillitten mange av informantene har til Google og Amazon ser ut til å være såpass stor at ingen tar seg bryet med å sette seg inn i personvernerklæringer, eller selskapets praksis rundt forbrukerdata. De antar at deres personvern blir ivaretatt på en måte som samsvarer med hva de anser som akseptabel oppførsel, eller normer, slik Nissenbaum beskriver (2010), og opplever det derfor som et brudd i den kontekstuelle integriteten når disse normene ikke overholdes.

En konklusjon så langt er at de fleste informantene ikke helt ser ut til å forstå kommersiell overvåking, og til tross for at de sier at personvern er viktig for dem, er det kun et fåtall som aktivt forsøker å beskytte personlig opplysninger. Dette kan med andre ord bety at brukere av IPA ofte ikke vet hva som blir samlet inn, solgt videre og hvordan det blir brukt til å påvirke dem. I neste kapittel vil jeg derfor analysere informantens holdninger til påvirkning og målrettet reklame.

6. Påvirkning

Analysens tredje dimensjon er påvirkning. Her vil teorien om overvåkingskapitalisme være i fokus, da det er selskapers analyse av menneskelig oppførsel som kan avsløre forutsigbar oppførsel (Zuboff, 2019, s. 8). Jeg vil se nærmere på hvordan informantene forholder seg til påvirkning gjennom teknologi. Til tross for at denne studien tar for seg IPA, er det viktig å ta i betraktning at flere faktorer kan spille inn på hvilke annonser du blir eksponert for. Både mobiltelefon, nettlogg, IPA, GPS, sosiale medier og andre enheter er en del av informasjonsalgoritmen. Likevel er dette kapittelet relevant i for problemstillingen, da dette belyser informantenes oppfatning av påvirkning gjennom algoritmer basert på deres «unyttige» informasjon, og rundt det å åpne opp for teknologiske enheter som samler informasjon, og bruker denne informasjonen til å påvirke.

Den første gangen jeg selv husker å ha blitt påvirket, var den dagen jeg så musikkvideoen til Britneys «Oops, I did it again». Alt hun hadde ville jeg også ha. Rommet mitt var fullt av Britney-plakater og jeg kan den dag i dag sangtekstene til samtlige av hennes 90- og tidlig 2000-tallsalbum. Etterhvert som jeg ble eldre vokste jeg ut av Britney-fasen, men jeg sluttet ikke å la meg påvirke av andre. Jeg ble påvirket av de eldre jentene på skolen, nye kjendiser, og venninnene mine. Alle gikk med de samme klærne og hørte på den samme musikken. Likevel var verden så liten på den tiden, uten sosiale medier og fri for kommersiell overvåking. Vår kilde til inspirasjon var ukemagasiner, MTV og hverandre.

Da jeg var yngre visste ikke butikker jeg handlet i hva jeg kom til å kjøpe neste gang, og jeg ble ikke eksponert for ting jeg «sannsynligvis kommer til å like». Butikkjeder håndplukket ikke produkter til meg, og jeg fikk ikke mail hver gang det kom en ny kolleksjon. Det får jeg i dag. Overalt er det butikkjeder som vil jeg skal handle. Rabattkoder gis over en lav sko, og alt er tilpasset min smak. Deres algoritmer kjenner meg bedre enn hva jeg gjør selv. Dette er overvåkingskapitalisme, og ifølge Shoshana Zuboff er dette en kamp mellom kapitalistene og oss. Hun mener det en innblanding i menneskets frie vilje, og en invasjon av vår selvstyrerett (Kavenna, 2019).

6.1. Holdninger til målrettet reklame

Kanskje den mest allmennkjente formen for overvåkingskapitalisme, er knyttet til personlig, målrettet reklame. Jeg vil aller først se nærmere på informantenes holdninger til dette

fenomenet. Er det noe unge mennesker i 20-årene er kjent med, på tvers av kulturelle forskjeller, kjønn, eller interesser? Informantene ble derfor spurt om de selv har opplevd å få personlig rettet reklame etter å ha snakket om et produkt, og dette er noe samtlige av informantene kunne bekrefte at de har opplevd. Mina har sluttet å la seg overraske:

> Jeg har opplevd å få personlig reklame så mange ganger at det ikke overrasker meg lenger når det skjer. Før kunne jeg reagere kraftig på det, og være sånn *«hæ, jeg snakket jo om dette i går, og nå får jeg reklame på det».* Nå er jeg bare sånn, *«ja, de finner ut av alt liksom.* (Mina)

Personlig rettet reklame er noe alle informantene kjenner godt til og har personlig erfaringer med. Med unntak av én informant, mottar alle informantene jevnlig reklame spesielt tilpasset deres interesser og hobbyer. Likevel har informantene svært delte holdninger til nettopp dette, hvor Thomas mener det er brukeres ansvar å sette seg inn i hvordan deres data blir brukt av tredjepartsaktører:

> Jeg tenker sånn, hvis du ikke kan teknologien, og kjøper en Goole Home eller Alexa, da får du godta det som skjer. Du kan ikke kjøpe sånt utstyr og være den som skriker høyest når du får reklame på Instagram. Da er det sånn, da får du lese den personvernserklæringen liksom. (Thomas)

Han mener likevel personlig reklame vært et irritasjonsmoment for han tidligere, og husker spesielt en episode hvor han og samboeren diskuterte puter til sofaen, hvor han fikk sosiale medier fullt av reklame på disse putene:

> Det var etter en episode når jeg og samboeren min snakket om puter til sofaen, og dagen etter hadde jeg alt av sosiale medier fullt av reklame fra den butikken, med fargene hun hadde nevnt. (Thomas)

For Thomas ble dette irritasjonsmomentet så stort, at han valgt å koble ut sin IPA:

> Jeg endte med å koble Alexa ut på grunn av det. Jeg kunne ikke snakke om et eneste produkt uten å få reklame på Facebook eller Instagram. Til og med nettaviser fikk jeg reklame hos. (Thomas)

Han mener i tillegg at denne reklamen kan være med å ødelegge overraskelser og gaver for personer man deler husstand med:

> Nå er vi jo nærme jul. Det hadde jo vært kjipt om jeg forteller noen hva jeg har kjøpt til samboeren min mens jeg sitter her hjemme i stua, så får plutselig hun masse reklame på akkurat det, helt ut av det blå. Det er jo mest sannsynlig det som hadde skjedd også. Det kan jo ta bort mye glede da, spesielt hvis man kjenner til AI, og skjønner hva som skjer. Mange kunne jo fort lest sånne tegn. (Thomas)

For Thomas ble altså personlig reklame et irritasjonsmoment, og bakgrunn for at han valgte å koble ut sin IPA. For over halvparten av informantene var målrettet reklame basert på personlig samtaler noe de hadde negative assosiasjoner til, og flere nevner dette som en grunn til å frakoble IPAen. Av totalt 11 informanter er det kun én som ikke mottar målrettet reklame. Josh forklarer at han har satt seg inn i hvilke enheter og applikasjoner som har evnene til å lytte til samtaler for å bruke dette i en kommersiell setting:

> I have received targeted ads before obviously, everyone has. But recently I do not, because I'm more on top of what's listening. So generally, my wife will get ads, but I don't, because I turned off ad-customization in google settings, and I have all the permissions on my phone locked down. (Josh)

Josh er nøye med hvem han gir tillatelse til å ha på mikrofonen, og da spesielt på telefonen sin. Han gjør endringer i tillatelser om han mot formodning mottar annonser som ser ut til å være målrettet:

> If I get a really targeted ad about something I was talking about, I will go back through my phone and look for whatever app I haven't revoked my microphone permissions from. I mean with my Google Homes, I know that they are there. But if I have an app on my phone or my laptop, that I don't know whether or not they are listening, I'm going to have to revoke that privilege and find out what is and what isn't. (Josh)

Josh passer dermed alltid på å tilegne seg nok informasjon om appene som muligens lytter til hva han sier, og er streng med hvilke apper som får tilgang til mikrofonen. På grunn av dette er han den eneste informanten som ikke mottar målrettet reklame. Men til tross for at mange har negative assossiasjoner til fenomenet, er det også informanter som ser det positive i målrettet reklame, og finner reklame mindre irriterende når det treffer på deres interesser og hobbyer. Sander setter pris på at han får med seg tilbud og tips innenfor hans interesseområder:

> Jeg merker jo det at reklame jeg får er relevant for meg da. Jeg er jo veldig opptatt av hudpleie, så jeg får jo masse reklame på det nå. Det er noe jeg bruker tiden min på. For min del går det helt fint med målrettet reklame, og jeg får jo relevant informasjon gjennom den reklamen. Jeg får jo tilbud og tips om nye produkter fra den og den. (Josh)

Sander mottar informasjon om nye produkter han ønsker å teste ut, og setter pris på tilbudene han får. Han ville ikke byttet ut målrettet reklame med tilfeldig annonser:

> Jeg vil jo ikke ha reklame på helt andre ting i stedet. Jeg vil ikke ha reklame på kattemat eller babyklær. Da vil jeg heller ha hudpleie, festivaler og sånne ting da. (Sander)

Også Eirik ser de positive sidene ved tilpasset reklame, og mener algoritmene som kan tilpasse hans annonser fungerer fint:

> Jeg tenker at når man først har de algoritmene som kan lage tilpasset reklame, om man da skal velge å få tilpasset eller få helt tilfeldig, så er det jo ikke bare negativt med å få tilpasset reklame til hva de tror behovet ditt er. Så, nei, jeg synes det er helt fint altså. (Eirik)

Eirik mener altså at ettersom man vil få reklame uansett, er det er fint med reklame som faktisk treffer forbrukeren. Det er dermed stor variasjon i informantenes generelle holdning til målrettet reklame. For Thomas har fenomenet vært grunn for å koble fra IPAen. For Josh er det viktig å ha kontroll på hvem som har mikrofontilgang, slik at han i stor grad unngår målrettet reklame. For Sander og Eirik er personlig reklame noe de har en generell positiv holdning til, da de mottar relevant informasjon til produkter de er interessert i.

6.2. Påvirkelighetsgraden

Det neste det blir naturlig å legge fokus på, etter å ha kartlagt at informantene er godt kjent med å få tilsendt målrettet reklame, eller hvorvidt de mener de selv er åpne for påvirkning av annonser. Ifølge Shoshana Zuboff (2019) er det nemlig mulig å endre en persons oppførsel gjennom sensorene i IoT-enheter. Ettersom sensorene plukker opp og analyserer data og menneskelig oppførsel kan leverandøren finne ut hvordan de kan endre dette i sitt favør (Zuboff, 2019, s. 292).

Zuboff beskriver denne påvirkningen som «tuning», hvor hun mener det blir sent subliminale hint til forbrukeren, skapt for å endre oppførselen til en person for maksimal innflytelse (Zuboff, 2019, s. 293). Hvordan subliminale hint i reklame faktisk kan ha en innflytelse har

vært mye omdiskutert. I 1957 ble det gjort et eksperiment i USA, hvor det ble vist slagord som «spis popcorn» og «drikk Coca Cola» gjennom en kinofilm. Klippet var langt nok til at underbevisstheten plukket det opp, men kort nok til at publikummerne ikke la merke til reklamen. James Vicary, som sto bak eksperimentet, hevdet at eksperimentet hadde økt salget av Coca Cola med 18.1%, og popcornsalget med 57,8%. Dette eksperimentet viste seg senere å være en bløff, og det hadde ikke faktisk hatt en merkverdig effekt på omsetningen (Love, 2011). BBC forsøkte senere å gjenskape eksperimentet, men dette hadde heller ingen betydelig effekt (BBC, 2015). I dag er det trolig ikke korte slagord som blir vist gjennom reklame, men heller små, subliminale hint som påvirker underbevisstheten til forbrukerne, slik Zuboff beskriver. Annonser vil som oftest ikke komme direkte gjennom IPAen til forbrukerne. De vil trolig dukke opp på deres sosiale medier-kontoer, nettaviser, og generelt når de benytter seg av internett. Derfor er det i dette kapittelet et fokus på hvorvidt de selv tror de er åpne for påvirkning gjennom reklame. Informantene ble spurt om de føler Google/Amazon kan påvirke dem til å handle. Taylor føler hun ofte kjøper ting hun får reklame på, og kjøper gjerne gjennom reklame tilpasset henne:

> When I see ads on my phone, there is so many times I buy things I don't need. If I see something that's cool, I'm such a consumer. So yeah, I definitely buy things from cool ads that pop up on my feed. (Taylor)

Taylor handler, ifølge henne selv, ofte utfra annonsene hun bli eksponert for. Hun sier dette skjedde så sent som dagen i forveien:

> I just did it yesterday. There's actually these jeans that I have been looking on since thanksgiving, and they keep popping up like here and there, and I just didn't buy them. And then they popped up again yesterday, so I bought them. Ads really have a big influence on me. (Taylor)

Taylor endte altså opp med å kjøpe buksene. I dette tilfelle er det en mulighet for at den hyppige og kontinuerlige eksponeringen kan ha hatt en påvirkende effekt på Taylors underbevissthet, som til syvende og sist gikk i selgerens favør. Også Brian innrømmer at han ofte faller for fristelsen, og blir påvirket av målrettet reklame mot han:

> Yeah, I mean of course. I think anyone who says no is kidding themselves. Like, when you see an ad for å burrito, and you want Mexican food that night. It's always correlations between that. (Brian)

Brian føler altså at det er en sammenheng mellom reklame man ser, og ting man har lyst på. Han stiller seg likevel positiv til påvirkningen det har, og handler gjerne etter å ha blitt eksponert for målrettet annonser. Han begrunner det med at han lar seg påvirke når det er ting han liker:

> Personally I don't mind targeted ads, I´ve bought a lot of stuff from targeted ads. I mean its targeted because its stuff I like. You don't have to deny that. It's not a bad thing to admit. They're not going to make me change who I am as a person, but like, maybe I would by a different brand or something. (Brian)

Som både Brian og Taylor illustrerer, er det lett å la seg påvirke av målrettet reklame. Enten om det er å kjøpe en bukse man i utgangspunktet ikke tenkte å bruke penger på, eller kjøpe meksikansk mat enda en gang denne uken, fordi man så det på sosiale medier. Mina er derimot mer skeptisk, og utrykker bekymring for hvor detaljert og påvirkningsfullt tilpasset reklame kan være:

> Jeg tenker jo, som kanskje er det skumleste... Si du får reklame på en spesifikk genser da, så har de allerede kartlagt at dette er trolig noe du har lyst på i utgangspunktet. Så da sitter de på tall på hvor mange ganger jeg har blitt eksponert for denne genseren, og eventuelt hvor mange ganger jeg har klikket meg inn på den, og når jeg eventuelt kjøper den. (Mina)

Hun stiller seg kritisk til hvor mye informasjon noe så uskyldig som det å kikke på et klesplagg kan avsløre. Hun tror kjedene kan beregne hvor ofte en person må eksponeres for noe, før han eller hun ender opp med å kjøpe det aktuelle produktet:

> Så da vet jo de hvor mange ganger jeg må eksponeres for noe de tror jeg vil like, før jeg ender opp med å kjøpe det. Det har jeg egentlig aldri tenkt over før, men det var sykt skummelt når jeg begynte å reflektere over det. (Mina)

Denne kartleggingen Mina snakker om, gjenspeiler hva Zuboff beskriver som «tuning», og er noe hun selv utrykker bekymring overfor når hun reflekterer over det. Informantene har altså god kjennskap til målrettet reklame, og mener dette har påvirket dem ved en eller flere anledninger. Særlig amerikanske informanter som Taylor og Brian ser ut til å stille seg mer positive til påvirkning av målrettet reklame. Brian tror ikke likevel ikke det har mulighet til å påvirke hvem han er som person. Dette mener derimot Shoshana Zuboff er mulig, og hun

mener små subliminale hint er hvordan overvåkingskapitalistene endrer forbrukerens oppførsel. Ta Brians situasjon som et eksempel, hvor han får lyst på meksikansk mat til middag på grunn av reklame. Kanskje har det vært implementert subliminale hint i annonsen som vekker hans kjøpelyst. Det kan også, ifølge tidligere studier, være forbruksvaner, som Verwimejeren et.al (2010) mener kan ha en innvirkende effekt på de subliminale hintene. Kanskje har Brian i løpet av dagen blitt eksponert for flere mat-annonser. Men dersom han har som vane å kjøpe meksikans mat, er dette noe han kanskje ville gjort uansett om han hadde blitt eksponert for annonsen eller ikke. Det er vanskelig å avgjøre hvorvidt det er subliminale hint som påvirker informantene, da det er stor uenighet hvorvidt subliminale hint kan bli brukt i markedsføring. Mens for eksempel Zuboff (2019), mener subliminale hint kan endre oppførsel, mener tidligere eksperimenter at det har liten merkverdig effekt (BBC, 2015). Verwimejeren et.al (2010) mener derimot at subliminale hint kan ha en effekt, men at faktorer som forbruksvaner vil ha en betydelig effekten på subliminale hint.

6.3. Politisk påvirkning

I starten av 2020 publiserte Forbrukerrådet en rapport kalt *«Out of Control: How consumers are exploited by the adtech industry - and what we are doing to make it stop"*. Rapporten handler om hvordan forbrukere av teknologiske enheter blir kontinuerlig overvåket, både på nett og i det virkelige liv, med en hensikt om å bli eksponert for målrettet reklame. Rapporten argumenterer for at aktørene i digital markedsføring utvikler detaljerte profiler til hver individuelle forbruker over tid, gjennom forskjellig enheter. Profilene blir brukt til både målrettet og personifisert reklame, men også til formål som diskriminasjon, manipulasjon og utnyttelse. Persondataen som samles inn gjennom apper selges så videre til andre aktører (Forbrukerrådet, 2020).

Wolfie Christl sin rapport går også inn på temaet om at vi blir kontinuerlig overvåket, og datainnsamlingen blir brukt i en markedsføringssammenheng. Han kommer også inn på temaet IoT (Internet of Things), som er en viktig del av IPA. Han påpeker at selv om mobiltelefonen fremdeles er den største enheten når det kommer til overvåking og datainnsamling, har vi i tillegg nye enheter som er tilkoblet nett, som bærbare enheter, smart-tv, målere, termostater, røykvarslere, kjøleskap, briller, tannbørster og leker (Christl, 2017). Da denne rapporten ble skrevet i 2017 var ikke stemmeaktivert smart-assistenter like utbredt som det er i dag, men rapporten hans beskriver likevel hvordan disse

IoT-enhetene sammen klarer å utvikle en enda mer detaljert og personlig profil av brukerne, og hvordan mennesker har lite alternativer til å motstå denne datainnsamlingen (Christl, 2017).

Informantene i denne studien er alle enig i at store selskaper som Google og Amazon, som får direkte tilgang til innsiden av hjemmene deres gjennom IPA, har muligheten til å påvirke dem i form av målrettet reklame. I tillegg mener flere av informantene at påvirkningen fra Google og Amazon potensielt også kan påvirke deres politiske eller religiøse syn. Sander tror at man kan bli påvirket i forkant av et politisk valg:

> De har nok mulighet til å påvirke mye mer enn reklame. Hvis man tenker politisk da, hvis jeg er litt sånn på kanten til hva jeg skal svare. Så blir jeg plutselig eksponert veldig mye på ett politisk parti. Og får masse informasjon på saker jeg bryr meg om. Da vil jeg jo regne med at sannsynligheten blir høyere for at jeg stemmer på de, enn noe annet da. Så ja, absolutt, det tror jeg. (Sander)

Han mener det da er viktig å være bevisst på påvirkningen, samtidig som han tror mye av eksponeringen påvirker underbevisstheten:

> Det er jo viktig å være bevisst på det. Og da er litt sånn, hvis man er klar over det og er bevisst på det, da går det kanskje bedre. Jeg tror mye av det ligger i underbevisstheten, og noe man ikke merker selv. (Sander)

Informant Mina tror usikre mennesker har lettere for å bli påvirket, og at det kan gå så langt som å påvirke menneskers verdenssyn i en retning selskaper bak algoritmene mener du bør ha:

> La oss si da, at jeg hadde vært en jævlig usikker sjel som er i tvil på hva man tror på. Da er det jo veldig lett å påvirke personen nok til å få et verdenssyn som de er enig i at du bør ha da. (Mina)

Michael mener amerikansk politikk er bevis på at folk blir påvirket av store selskaper. Han mener store selskaper har for stor makt i amerikanske husholdninger, men ser ikke hvordan det skal være mulig å løse:

> Have you been following the politics here in America? So the answer is yes. I feel that large multi-billion dollar corporations have a little bit too much of a strong hold, or too much of a

> strong placement in the US household, US influence, all of the above, but I don't foresee how that could possibly be changed, so.. here we are. (Michael)

Michael mener disse multimilliardær-selskapene har for mye makt, og at de kan ha politisk påvirkning. Et slikt tilfelle har vært mye omdiskutert etter USAs presidentvalg i 2016, hvor Cambridge Analytica jobbet med Donald Trumps presidentkampanje, og hevder å ha påvirket valget i Trumps favør (Press, 2018). Selskapet samlet inn informasjon fra 87 millioner Facebook-profiler uten deres samtykke, og Alexander Nix, Cambridge Analyticas tidligere sjef, hevdet at de hadde kartlagt personlighetsegenskapene til alle voksne personer i USA (Press, 2018). Deretter fikk personer målrettet reklame som spilte særlig på frykt og følelser, basert på deres personlighetstype (Press, 2018).

6.4. Oppsummering

Samtlige av studiens informanter kjenner til konseptet målrettet reklame, og mange lar seg ofte friste til å kjøpe produkter. Det er stor variasjon i informantenes holdning til målrettet reklame. Noen foretrekker reklame basert på egne interesser fremfor annet reklame, mens det er et irritasjonsmoment for andre. Hvorvidt det er subliminale hint eller forbruksvaner som påvirker forbrukeren mest er usikkert, da det er stor uenighet hvorvidt subliminale hint kan bli brukt i markedsføring. Studiens informanter, uavhengig av kulturelle forskjeller, mener store selskaper som Google og Amazon har mulighet til å påvirke også politiske og religiøse valg, og dette fremkaller en negativ holdning hos informantene. Sander mener det er viktig å være bevisst på mulig påvirkning, men at han samtidig tror at påvirkningen skjer underbevisst, noe som tidligere har vært diskutert som subliminale hint. I tillegg beskriver Zuboff noe hun kaller for «choice arcitecture», som kan oversetter til «valgarkitektur». Begrepet referer til hvordan situasjoner allerede er strukturert for å tilegne seg oppmerksomhet og påvirke handling (Zuboff, 2019, s. 293). Og dette ser informantene ut til å reflektere over, eksempelvis Mina, som foreslår at mennesker som ikke er sikre på hva de tror på, kan bli påvirket til å adoptere verdenssynet de blir eksponert for gjennom annonser. Hvor mye forbrukere velger å bruke sin IPA vil naturligvis ha en effekt på hvor mye informasjon enheten klarer å hente inn. Ifølge West (2019), tilbyr IPAer å tjene oss ved å kjenne oss. Assistenten lærer å kjenne forbrukeren gjennom *hva* man sier, og *hvordan* man sier det. Samtidig som IPAen blir en pålitelig del av hverdagen, blir overvåkingen fra et enormt selskap normalisert gjennom den varme personligheten til assistenten (West, 2019). I neste kapittel vil jeg derfor analysere informantenes holdninger til assistentens menneskelig egenskaper og kvinnelig fremtoning.

7. Menneskelig egenskaper (antropomorfisme)

Antropomorfisme betyr å tilegne menneskelig egenskaper, som motivasjoner, intensjoner og følelser, til et ikke-menneskelig objekt (Epley, Waytz, & Cacioppo, 2007). Dette kan for eksempel være å si at solen smiler, himmelen gråter, eller havet er tålmodig (Haugen, 2019). Det er ofte å se i fantasyfilmer, barnelitteratur og animasjonsfilm. For eksempel i mange av Disneys filmer utspilles menneskelig drama med dyr i hovedrollene. I Narnia-universet kan noen dyr både tenke og snakke, mens andre dyr er «bare» dyr (Haugen, 2019). Antropomorfisme skjer ofte når objektet har visse egenskaper som likner et menneske (Cao, Zhao, & Hu, 2019), og det er her det er interessant å se nærmere på IPAens feminine kvaliteter.

Ifølge Heater Susanne Woods (2018) er den feminine fremtoningen i IPA med på å skape en trygghet i hjemmet, og øke bruken av assistenten. Hun foreslår derfor at den feminine fremtoningen i en IPA begrunnes i stereotypiske kjønnsroller, hvor kvinnen blir sett på som en omsorgsperson, eksempelvis en mor eller kone. Dette for å skape et forhold mellom enheten og forbrukeren, slik at skepsisen til selskapene bak viskes ut, og man inviterer overvåkingen inn på et mer intimt plan. (Woods, 2018) Hensikten med denne dimensjonen er å se nærmere på om det er en sammenheng mellom den kvinnelige fremtoningen til assistenten, og forbrukernes holdninger til overvåking og personvern.

Jeg forestiller meg ofte ansikt til stemmer jeg kun hører, og tidligere forskning viser at nettopp stemme en sterk indikator som trigger antropomorfisme (Cao, Zhao, & Hu, 2019). Jeg har nemlig alltid sett for meg at min Google Assistant ser ut som skuespiller Lori Loughlin. En blid og vennlig dame med karamellblondt hår. Siri ser i mitt hode ut som en nordisk kvinne med kortklipt lyst hår, og Alexa er en kvinne med skulderlangt mørkt hår. For meg er det ganske tydelig hvordan disse ikke-menneskelig assistenten ser ut, til tross for at stemmene deres er ganske like. Jeg føler ikke at jeg snakker til et menneske når jeg snakker til assistenten, men jeg har likevel tilegnet den et menneskelig utseende, eller en egenskap, og det er dette som er antropomorfisme. Begrepet antropomorfisme brukes ofte om hverandre med begrepet personifisering (Pradhan, Findlater, & Lazar, 2019). IPAer kommer ofte med både kvinnelig stemme og navn. Det kan derfor argumenteres for at IPAen benytter seg av en kvinnelig personifisering.

Mennesker skaper ofte et forhold til, og gir menneskelig egenskaper til tingene vi bruker tid sammen med. Vi navngir for eksempel båter, biler og andre ting i livene våre, og noen føler en sterk tilknytning til disse tingene (Coughlin, 2018). Forskjellen mellom andre objekter vi knytter oss til, og IPA, er at disse enhetene ofte plasseres i flere rom i hjemmet, slik at de lærer av oppførselen vår, og blir en pålitelig del av hverdagen (Coughlin, 2018). Denne interaktive samhandlingen med en ikke-menneskelig assistent inneholder flere av nøkkelelementene i et forhold, og dermed har de evnen til å spille rollen som en sosial partner (Coughlin, 2018). Som nevnt innledningsvis ville jeg trolig aldri gått med på å slippe et selskap som Google inn i hjemmet mitt med en alltid-lyttende mikrofon. Men når det kom maskert som en vennlig assistent, forsvant denne skepsisen. For å se nærmere på hvorvidt det finnes en sammenheng mellom IPAens antropomorfisme, og informantenes holdning til overvåking og personvern, vil jeg først kartlegge hvor mange informanter som faktisk har en IPA med kvinnelig stemme:

7.1. Den digitale fremtiden er kvinne

Nedenfor er det presentert en tabell som viser hvilken stemme hver informant har/har hatt på sin IPA, og det er en tydelig overvekt av kvinnelig stemme. Det er kun én informant av totalt 11, som har mannsstemme:

Informant	**IPA med manns-/kvinnestemme**
Thomas	Kvinne
Mina	Kvinne
Eirik	Mann
Sara	Kvinne
Ole	Kvinne
Sander	Kvinne
Rachel	Kvinne
Taylor	Kvinne
Josh	Kvinne
Brian	Kvinne
Michael	Kvinne

Eirik er den eneste av informantene som har en IPA med mannsstemme. Han sier at han ikke husker helt hvorfor han valgte nettopp dette:

> Jeg har mannlig stemme på min, men jeg husker ikke helt hvorfor. Det er vel en del ulike stemmer du kan velge mellom, men jeg har egentlig ikke orket å rotet så mye med akkurat det. (Eirik)

Han begrunner det selv med at han ikke har rotet noe særlig med valgene rundt IPAens stemme, og det kan heller ikke tolkes som at Eirik har noe problem med å ha en mannlig stemme. Eirik var i tillegg den eneste informanten fra Norge som *ikke* nevner mulig overvåking som en negativ side ved IPA. Samtlige av de amerikanske informantene har kvinnelig stemme på sin IPA, og dette begrunner de med at de beholdt standard-innstillingen slik den var. Amazon med sin Alexa gir ikke muligheten til å endre assistentens kjønn på samme måte som Google gjør, og dermed har de som eier en Alexa ikke tatt et bevisst valg rundt ønsket stemme. Det er likevel mulig for Amazon Alexa-brukere å laste ned enkelte kjendisstemmer, som Samuel Jackson til å for eksempel fortelle vitser o.l. (Amazon). Informantene fra USA var langt mindre skeptiske til overvåking fra IPAen, i forhold til de norske informantene. Derfor vil jeg nå se om det finnes en sammenheng mellom assistentens stemme, og de norske informantenes skepsis.

7.1.1. «Det føles tryggere.»

Hjemmet skal føles trygt, og som diskutert tidligere, er den største frykten i forhold til IPA hos norske informanter, uvissheten hvorvidt assistenten tjuvlytter til samtaler, og overvåker forbrukeren. Informant Sara valgte å koble fra sin IPA av flere årsaker, hvor en av dem var frykten for å si noe «feil» i sitt eget hjem, og risikere at assistenten plukket opp dette. Hun hadde Amazon Alexa, og derfor kvinnelig stemme på sin IPA. Hun tror kvinnelig stemme føles tryggere enn en mannsstemme:

> Jeg tror kvinnestemmer er litt mer varme, litt mer trygge. Selv om den gjør den samme jobben, så oppfattes mannsstemme litt mer truende da. Men det kan jo hende menn er annerledes da, at det ikke føles like inntrengende å ha en mannsstemme om man er mann selv. Kanskje man bare foretrekker det som virker mest kjent for en selv. (Sara)

Sara oppfatter altså kvinnestemme som litt mer varm og trygg i forhold til en mannsstemme, og ifølge tidligere studier, er det nettopp denne stereotypiske ideen om at kvinnen er en

omsorgsperson, som er bakgrunn for IPAens feminine fremtoning (Woods, 2018). I tillegg foreslår Sara at man kanskje velger den stemmen man selv er mest kjent med, eller er av samme kjønn som en selv. Dette ser, utfra informantutvalget ikke ut til å være tilfelle. Alle mennene, med unntak av én, har kvinnelig stemme, uavhenig om IPAen tilbyr mansstemme eller ikke. Dermed er det lite i studien som tyder på at forbrukere velger den stemmen de er mest kjent med selv, ettersom informantene med en IPA som også tilbyr mannsstemme, stort sett velger kvinnelig stemme. Også den andre norske, kvinnelig informanten, Mina, føler det er tryggere med en kvinnelig stemme. Hun har Google Home, og dermed muligheten til å endre til mannsstemme:

> Jeg husker veldig godt at vi testet mannsstemme, men det ble så rart. Jeg føler det skal være en kvinnestemme. Og jeg tror det føles mindre inntrengende å ha en kvinnestemme som snakker til deg da. Så vi valgte kvinnestemme fordi det bare føltes mer betryggende. (Mina)

Begge de norske, kvinnelig informantene føler seg tryggere med en kvinnelig stemme. Som Woods (2018) foreslår, er den kvinnelige fremtoningen med på å skape en trygghet i hjemmet, og dette ser ut til å appellere til begge informantene.

7.1.2. Stereotypiske kjønnsroller

De mannlig, norske informantene som har tatt et bevisst valg rund stemmen til sin IPA, oppgir ikke økt trygghetsfølelse som begrunnelse. Hos disse informantene derimot, er det stereotypiske kjønnsroller, hvor kvinnen blir forbundet med serviceyrker, som ser ut til å ha vært en avgjørende faktor. Sander er en av informantene som har tatt et bevisst valg om å ha kvinnelig stemme. Bakgrunnen er at det stemmer overens med bildet han har av en assistent:

> Jeg har valgt å ha kvinnestemme fordi jeg det er sånn en assistent skal høres ut. Jeg kunne ikke tenkt meg å ha mannsstemme, og jeg vet ikke helt hvorfor. Kanskje det er på grunn av filmer og sånne ting, der føler jeg alltid at assistenten er kvinne. Det er bare sånn jeg tenker at den skal høres ut. (Sander)

Sander tenker altså at den kvinnelige stemmen er hvordan en assistent skal høres ut, og tror dette kan skyldes filmer, hvor assistenter ofte blir spilt av en kvinne. Tidligere studier viser også at kvinner er det foretrukne kjønn i yrker som assistent/sekretær (Heilman & Eagly, 2008). Thomas føler Alexa er en kvinne:

> Kvinnestemme var standard når jeg satte den opp, så det var liksom Alexa sin stemme, og jeg vil jo si at Alexa er en kvinne. (Thomas)

Thomas føler i tillegg det er lettere å skape et slags forhold til en kvinnelig stemme, fremfor en mann, når man ikke har et forhold til stemmen i utgangspunktet:

> Og man kan jo få stemmen til kjendiser og da ville jeg ikke brydd meg så mye om det er en mann eller kvinne. Men hvis man skal ha stemmen til en vanlig fyr på gata på høyttaleren ville vært rart. Jeg vet ikke, det er kanskje lettere å skape et forhold til en kvinnelig stemme, enn en mannlig stemme når man ikke har noe forhold ellers til denne stemmen. (Thomas)

I tillegg til å omtale Alexa som hunkjønn, mener Thomas det faller mer naturlig å omtale materialistiske ting som hunnkjønn:

> Folk kaller jo, eller gir bilen eller båten sin et kjønn, og da er det jo alltid hun. Det er jo aldri *han* bilen. Eller *han* båten. (Thomas)

Flere av informantene velger å omtale assistenten som «hun/she», og tilegner assistenten en menneskelig egenskap, for eksempel kjønn. Eirik derimot, som har mannsstemme, er svært bevisst på at assistenten hans er en forlengelse av Google, og ikke en menneskelig assistent.

> Jeg tenker at det er en liten assistent, men jeg har ikke gitt den noe menneskelig egenskaper. Jeg tenker at Google er Google. Så det er ikke noe levende, men heller bare et hjelpemiddel i hjemmet. (Eirik)

Også Thomas er klar på at det er en søkefunksjon, eller en enhet som kan gjennomføre enkle oppgaver på hans kommando. Han mener likevel at den kvinnelig stemmen til Alexa har en betryggende følelse fordi det kan minne om en omsorgsfull kvinne:

> Når jeg snakker med høyttaleren, så tenker jeg at jeg kommuniserer med noe som kan søke på vegne av meg, men ikke at jeg snakker med en dame som heter Alexa. Men jeg liker bedre å ha en damestemme, og det kan jo være på måte sånn, alle har en mor, og man er vandt til at en kvinne er litt autoritær, men også en omsorgsfull person, og man søker jo omsorg rundt seg. (Thomas)

Til tross for at han ikke ser for seg at han snakker med en ekte kvinne når han snakker med Alexa, tror han altså at stemmen har en betryggende effekt i søken etter omsorg.

7.2. Frykten for overvåking og følelsen av trygghet

De amerikanske informantene har alle kvinnelig stemme. De ga samtidig lite refleksjoner hvorvidt de foretrakk kvinnelig stemme overfor en mannsstemme. Samtlige av de amerikanske informantene hadde behold standard-innstillingen, som er kvinnelig. Majoriteten av de norske informantene har derimot reflektert rundt hvorfor de er mest komfortable med en kvinnelig assistent, fremfor en mannlig. Av norske informanter er det også flere som har Google Home, fremfor Amazon Alexa. Google gir større valgmuligheter til å endre assistentens kjønn og stemme, men dette ser ikke ut til å ha en merkverdig effekt på hva forbrukerne til syvende og sist foretrekker. Både kvinner og menn ser ut til å foretrekke den kvinnelig versjonen, uavhengig av hvilken grad enheten tilbyr valgmuligheter, og begrunnelsen kan deles opp i to grupper, hvor informantenes kjønnsforskjeller ser ut til å være et nøkkelelement. De kvinnelig informantene, Sara og Mina, foretrekker kvinnelig stemme basert på en økt trygghetsfølelse i hjemmet. Dette har dog ikke gitt nok trygghetsfølelse for Sara, som likevel får en overvåkingsfølelse av å ha sin IPA tilkoblet, uavhengig av kjønn, og har derfor tatt det valget om å koble assistenten ut permanent. Mina har prøvd med mannlig stemme, men dette har altså ikke gitt henne den samme betryggende. De mannlig informantene derimot, velger kvinnelig assistent basert på bildet de har av hvordan en assistent skal høres ut. Begge gruppene kan sammenliknes med tidligere studier, hvor den feminine fremtoningen til en IPA, er nøye utformet for økt trygghetsfølelse i hjemmet, i tillegg til å spille på stereotypiske kjønnsroller (Woods, 2018).

7.3. Oppsummering

Av norske og amerikanske informanter, er det kun de norske informantene som reflekterer rundt hvorfor de foretrekker kvinnelig stemme i sin assistent. Til tross for at Google Home gir større valgmuligheter når det gjelder IPAens kjønn, ser ikke dette ut til å ha en merkverdig effekt på hva informantene foretrekker. Både kvinner og menn foretrekker stort sett kvinnelig stemme, men de ser ut til å foretrekke kvinnelig stemme av forskjellig årsaker. Kvinner utrykker at de får økt trygghetsfølelse av en IPA med kvinnelig stemme, mens menn føler det er slik en assistent skal høres ut, noe som kan antyde at stereotypiske kjønnsroller i samfunnet, også kan overføres til teknologien.

Både de kvinnelige og mannlige informantene fra Norge svarte derimot også at de anser overvåking som IPAens største ulempe. Likevel er det bare Sara og Thomas som har tatt

valget om å koble assistenten fra. Derfor kan det argumenteres for at til tross for at forskere mener vi utsetter oss for overvåking fra et enormt selskap, blir det normalisert gjennom den varme og kjente personligheten som er blitt tilegnet selskapene gjennom deres IPA (West, 2019). Til tross for at selskapet og tjenesten er den samme, uavhengig av «kjønn» til assistenten, kan det se ut til at den feminine fremtoningen til assistenten i flere tilfeller visket ut skepsisen flere av informantene ser ut til å ha rundt det å invitere overvåkingen inn på et mer personlig plan. Det er tross alt de norske informantene som i større grad frykter overvåking fra IPA, samtidig som det også er denne gruppen som trekker frem ord som «betryggende», «vennlig», «varm», og «det er sånn en assistent høres ut», når de omtaler assistenten. Dette kan være en indikasjon på at selskapet suksessfullt har distansert seg nok fra IPAen i tilfeller hvor forbrukere frykter kommersiell overvåking, og at forbruker nærmest ser leverandør og assistent som to uavhengige tjenester.

8. Oppsummering og konklusjon

Denne komparative, kvalitative studien tar for seg unge menneskers forhold til personvern og overvåking i bruken av intelligente personlig assistenter, også kjent som smarthøyttalere. Studiens problemstilling er som følger:

> *Hvilke refleksjoner har brukere av intelligente personlig assistenter rundt personvern og overvåking?*

I studiens analyse har jeg tatt utgangspunkt i følgende dimensjoner: overvåking, personvern, påvirkning, og IPAens menneskelig egenskaper (antropomorfisme). Gjennom 11 kvalitative intervjuer med informanter fra både Norge og USA, har jeg på denne måten sett nærmere på hvordan unge mennesker i alderen 20-29 år forholder seg til, tolker og reflekterer rundt overvåking, personvern, påvirkning og antropomorfisme i forbindelse med en IPA. Disse talestyrte enhetene med en alltid-tilkoblet mikrofon er ikke nødvendigvis det avgjørende elementet i om personer blir overvåket og ikke klarer å beskytte eget personvern. Likevel mener jeg det representerer en normalisert aksept rundt det å invitere overvåkingskapitalismen inn på et mer personlig plan, og det er derfor viktig å se på forholdet mellom enhet og forbruker. Nye teknologier med datamediert kommunikasjon kommer inn i livene våre med apper, enheter og tilkoblinger. Vi blir distrahert av suksessen fra den høyst bevisste overvåkingskapitalismen, og risikerer til syvende og sist å sitte igjen med en følelse av hjelpeløshet (Zuboff, 2019, s. 342).

I denne studien kommer det frem at det er blant informantene er en felles forståelse av fenomenet overvåking, på tvers av kulturer. Flere trekker frem at overvåking er et negativt ladet begrep, eller at de får negative assossiasjoner til fenomenet. Det er altså lite som tyder på at fenomenet overvåking blir oppfattet annerledes i USA enn i Norge. Det kommer dog frem at flere informanter over 25 år trekker frem situasjoner hvor de anser overvåking som et positivt virkemiddel dersom situasjonen tilsier det. Terror og kriminalitet blir brukt som hovedargumentet. Informantene over 25 år har muligens noe bedre minne av terrorangrepet 9/11. Til tross for at de nå er i relativt lik aldersgruppe, var det en langt mer merkverdig aldersforskjell 10- og 20 år tilbake i tid. Det er nemlig mange som regner 9/11 som startskuddet til sikkerhetsmessig overvåking (Mathiesen, 2013, s. 63), og dette kan være en av grunnene til at de eldste informantene også har denne holdningen. Derfor mener jeg det kan

ha en sammenheng mellom informantenes alder, og en mer positiv holdning til overvåking av sikkerhetsmessig årsaker.

Informantene forholder seg til fenomenet overvåking, og nettopp overvåking er noe de norske informantene frykter fra sin IPA. Denne frykten gjenspeiles ikke hos de amerikanske informantene. I tillegg er kun et fåtall som nevner kommersiell overvåking. Det kan derfor se ut til at det generelt er en manglende forståelse for fenomenet overvåkingskapitalisme, og hvordan dette foregår i praksis. I stedet frykter de overvåking fra statlig institusjoner, og flere er redd for å si noe feil i sitt eget hjem, og havne i politiets søkelys. Hvorfor flere norske informanter er av den oppfatning at politiet når som helst kan få tilgang til IPA-opptak kommer ikke frem i studien, men det ville utvilsomt vært spennende å se nærmere på.

Informantene har en generell holdning til at personvern er viktig. Her er det unge, norske menn som skiller seg ut fra øvrige informanter som mindre kritiske til hvor og hvem de deler informasjonen sin med. Det er likevel ingen som har lest IPAens personvernerklæring, og de aller fleste er ikke klar over hvordan deres persondata blir håndtert av IPAens leverandør i praksis. Av 11 informanter er det kun tre personer, hvorav to er fra USA og en fra Norge, som viser til spesifikke grep de tar for å beskytte eget personvern. Det er et paradoks at informantene sier at personvern er viktig for dem, samtidig som det kun er et fåtall som aktivt forsøker å beskytte personlig opplysninger. Dette kan med andre ord bety at brukere av IPA ofte ikke vet hva som blir samlet inn, solgt videre og hvordan det blir brukt til å påvirke dem.

Tillitten informantene har til IPAens leverandør viser seg å være stor. Denne generelle tillitten kan se ut til å bunne ut i at de anser fallhøyden som større for et stort selskap dersom de ikke håndterer personlig informasjon godt nok, noe som resulterer i at informantene ser det som usannsynlig at informasjonen deres blir misbrukt.

Informantenes ser ut til å ha en forventning til hvordan leverandøren håndterer deres persondata, og flere ble derfor overrasket da de ble gjort oppmerksomme på enkelte av funksjonene som blir praktisert av leverandør. For eksempel at menneskelig ansatte ved selskapet kan gå gjennom vilkårlige lydopptak, eller at deres samtaler med IPAen lagres permanent med mindre de selv skrur av funksjonen. Disse funksjonene ble oppfattet som brudd på personvernet av flere informanter fra både Norge og USA. Informantene reflekterer svært to-delt når det gjelder hva de tror er begrunnelsen bak menneskelig avlytting og lagring

av interaksjoner med assistenten. Samtlige av de norske informantene mener dette har med forbedring av brukeropplevelse, eller markedsføring, å gjøre. Men dette blir ikke nevnt av en eneste amerikaner. Av informantene fra USA sier tre av fem at de ikke kan komme på noen grunn for at det skal være en funksjon, én mener det er for leverandørens fordel, men usikkert hvordan, og siste er som Josh sier, fordi det er din stemme som blir tatt opp.

Samtlige av informantene har erfaringer med fenomenet, og flere sier de ofte bli påvirket til å handle gjennom målrettede annonser. De eldre informantene mot slutten av 20-årene ser ut til å ha et noe mer negativt forhold dette fenomenet, hvor flere har skrudd av sin IPA, og andre er nøye med hvilke apper og enheter de gir mikrofontilgang til. Informanter fra både Norge og USA mener også at store selskaper som Google og Amazon har mulighet til å påvirke også politiske og religiøse valg, og dette fremkaller en negativ holdning hos informantene. Her blir amerikansk politikk trukket frem som et eksempel, og slik politisk påvirkning gjennom målrettede annonser er noe som mottok stor oppmerksomhet i 2016, i den kjente Cambridge Analytica-skandalen (Press, 2018).

Når det gjelder antropomorfisme (ikke-menneskelig objekter med menneskelig egenskaper), og assistentens kjønn, har de norske informantene langt flere tanker og refleksjoner på hvorfor de er mest komfortable med en kvinnelig IPA. Ingen av de amerikanske informantene ser ut til å ha hatt et bevisst valg rundt dette, noe som også kan skyldes at majoriteten av de amerikanske informantene har Alexa, en IPA som ikke tilbyr en mannlig versjon på lik linje som Google. I Norge derimot, hvor Google er den mest populære IPAen, har informantene klare argumenter for hvorfor de ønsker en kvinnelig assistent. Både kvinner og menn ser ut til å foretrekke den kvinnelige versjonen, uavhengig av hvilken grad enheten tilbyr valgmuligheter, og begrunnelsen kan deles opp i to grupper, hvor informantenes kjønnsforskjeller ser ut til å være et nøkkelelement.

De kvinnelig informantene ønsker en kvinnelig assistent basert på økt trygghet i hjemmet, mens de mannlig informantene ønsker en kvinnelig assistent basert på stereotypiske kjønnsroller, og hvordan de ser for seg at en assistent skal høres ut. De fleste informantene fra Norge svarte også at de anser overvåking som IPAens største ulempe, noe som ikke var en gjentakende faktor hos de amerikanske informantene. Likevel ser det ut til at de norske informantene i større grad bruker antropomorfisme i beskrivelsen av IPA, og trekker frem ord som «betryggende», «vennlig», «varm», og «det er sånn en assistent høres ut», når de omtaler

assistenten. Dette kan være en indikasjon på at selskapet suksessfullt har distansert seg nok fra IPAen i tilfeller hvor forbrukere frykter kapitalistisk overvåking, og at forbruker nærmest ser leverandør og assistent som to uavhengig tjenester.

8.1. Konklusjon

Denne studien kan dermed konkludere med at norske informanter i større grad evner å reflektere rundt overvåking og personvern i bruken av intelligente personlig assistenter, hvor noen har valgt å koble sin IPA ut, på grunn av en kritisk holdning til informasjonsinnhenting eller målrettet reklame. De er mer kritiske til hva en IPA faktisk får med seg og samler inn av informasjon, og tror lagringsfunksjonen er basert på markedsføring. I tillegg har de norske informantene tatt et bevisst valg på hvilket kjønn de ønsker at assistenten skal ha, og dette valget blir tatt basert på trygghet av kvinner, og stereotypiske kjønnsroller av menn.

Informantene fra USA kan sies å ha et mer avslappet forhold til bruken av IPA. Her er det kun én informant som trekker frem mulig overvåking som en ulempe, mens resterende informanter trekker frem dårlig internett under orkansesong, eller at en IPA har liten nytte dersom man ikke har smart-hjem. Det er heller ingen informanter fra USA som har noe forhold til assistentens stemme. De norske informantene er klare på hvorfor de ønsker kvinnelig assistent, mens dette er ikke noe de amerikanske informantene reflekterer rundt.

Til tross for at norske informanter i større grad reflekterer rundt personvern og overvåking i bruken av IPA, ser det ut til å være en manglende forståelse for kommersiell overvåking, både hos de norske og amerikanske informantene. Det er et paradoks at personvern er noe informantene sier er viktig for dem, samtidig som det viser seg at de færreste tar aktive grep for å beskytte personlig informasjon.

Bibliografi

Agarwal, R. (2020, 02 21). *15 Examples of Artificial Intelligence You´re Using in Daily Life*. Retrieved from Beebom: https://beebom.com/examples-of-artificial-intelligence/

Alase, A. (2017, Februar 27). *The Interpretative Phenomenological Analysis (IPA): A Guide to a Good Qualitative Research Approach*. Retrieved from IJELS: https://www.journals.aiac.org.au/index.php/IJELS/article/viewFile/3400/2797

Ali, S., & Yusuf, Z. (2018). *Mapping the Smart Home Marked.* Hentet fra The Boston Consulting Group: https://image-src.bcg.com/Images/BCG-Mapping-the-Smart-Home-Market-Oct-2018_tcm56-204487.pdf

Amazon. (n.d.). *"Alexa, introduce me to Samuel L. Jackson"* . Retrieved from Amazon: https://www.amazon.com/b?ie=UTF8&node=20591210011

Anderson, M. (2017, Mai 05). *Burger King's Ad Exposed Voice Assistants' Hackability*. Retrieved from Inc: https://www.inc.com/associated-press/burger-king-ad-voice-assistants-siri-alexa-google.html

Atlam, H. F., & Wills, G. (2019, Mars). *IoT security, privacy, safety and ethics.* Retrieved from ResearchGate: 10.1007/978-3-030-18732-3_8

BBC. (2015, Januar 20). *Does subliminal advertising actually work?* Retrieved from BBC News: https://www.bbc.com/news/magazine-30878843

Berghel, D. H. (2018). *Malice Domestic: The Cambridge Analytica Dystopia.* Retrieved from IEEE: http://www.berghel.net/col-edit/out-of-band/may-18/oob_5-18.pdf

Bjørkeng, P. K. (2019). *Kunstig Intelligens; den usynlig revolusjonen.* Oslo: Vega Forlag AS.

Braut, G. S. (2020, Mars 12). *pilotstudie.* Retrieved from Store norske leksikon: https://snl.no/pilotstudie

Buchholz, K. (2021, Januar 15). *The Most Popular Smart Speakers in the U.S.* Retrieved from Statista: https://www.statista.com/chart/23943/share-of-us-adults-who-own-smart-speakers/

Burke, M. (2019, November 02). *Amazon's Alexa may have witnessed alleged Florida murder, authorities say*. Retrieved from NBC news: https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621

Campbell, J. E., & Carlson, M. (2002). *Panopticon.com: Online Surveillance and the Commodification of Privacy*. Retrieved from Journal of Broadcasting & Electronic Media: https://doi.org/10.1207/s15506878jobem4604_6

Cao, C., Zhao, L., & Hu, Y. (2019, Juni 15). *Anthropomorphism of Intelligent Personal Assistants (IPAs): Antecedents and Consequences Antecedents and Consequences.* Retrieved from AIS Electronic Library: https://core.ac.uk/reader/326833380

Christl, W. (2017, juni). *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade and Use Personal Data on Billions*. Retrieved from Creacked Labs: https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Cinnamon, J. (2017, Desember). *Social Injustice in Surveillance Capitalism*. Retrieved from ResearchGate: 10.24908/ss.v15i5.6433

Coughlin, J. (2018, September 23). *"Alexa, Will You Be My Friend? When Artificial Intelligence Becomes Something More*. Retrieved from Forbes: https://www.forbes.com/sites/josephcoughlin/2018/09/23/alexa-will-you-be-my-friend-when-artificial-intelligence-becomes-something-more/#9bebdf65c81f

Dahlum, S. (2021, Mars 09). *validitet.* Retrieved from Snl: https://snl.no/validitet

Datilsynet. (2018, Mai 29). *Om personopplysningsloven med forordning og når den gjelder*. Retrieved from Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/

Day, M., & Drozdiak, N. (2019, April 11). *Amazon Workers Are Listening to What You Tell Alexa*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

Drabløs, Ø. T. (2018, Oktober 09). *Advarer mot Googles norske smarthøyttaler: – Du må forstå konsekvensene for familiens personvern*. Retrieved from NRK: https://www.nrk.no/kultur/advarer-mot-googles-norske-smarthoyttaler_-_-ikke-en-hvilken-som-helst-husgjest-1.14239760

Epley, N., Waytz, A., & Cacioppo, J. T. (2007). *On seeing human: A three-factor theory of anthropomorphism.* Retrieved from Psychological Review: https://doi.org/10.1037/0033-295X.114.4.864

Forbrukerrådet. (2020, januar 14). *Out of Control: How consumers are exploited by the online advertising industry.* Retrieved from Forbrukerrådet: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

Gandy, O. H. (2011, april). *The Political Economy of Personal Information: The handbook of political economy of communication*. Retrieved from ResearchGate: 10.1002/9781444395402.ch20

Gentikow, B. (2005). *Hvordan utforsker man medieerfaringer?* . IJ-forlaget.

Grønmo, S. (2020, Oktober 07). *bias i forskning.* Retrieved from Snl: https://snl.no/bias_i_forskning

Haugen, M. O. (2019, September 22). *antropomorfisme*. Retrieved from SNL: https://snl.no/antropomorfisme_-_litteratur

Heilman, M. E., & Eagly, A. H. (2008). *Gender Stereotypes Are Alive, Well, and Busy Producing Workplace Discrimination.* Retrieved from Industrial and Organizational Psychology: https://library.pcw.gov.ph/sites/default/files/gender%20stereotypes%20are%20alive.pdf

hifiklubben. (u.å). *Stemmestyring "Siri, Google Assistant og Alexa*. Retrieved from Hifi klubben: https://www.hifiklubben.no/inspirasjon/streaming/stemmestyring/

Kavenna, J. (2019, oktober 04). *Shoshana Zuboff: "Surveillance Capitalism is an assault on human autonomy"*. Retrieved from The Guardian: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

Khan, M. A., & Salah, K. (2018, Mai). IoT Security: Review, blockchain solutions, and open challenges. *Elsevier*, ss. 395-411.

Kinsella, B. (2019, Juni 21). *Voice Assistant Demographic Data – Young Consumers More Likely to Own Smart Speakers While Over 60 Bias Toward Alexa and Siri* . Retrieved from Viocebot.ai: https://voicebot.ai/2019/06/21/voice-assistant-demographic-data-young-consumers-more-likely-to-own-smart-speakers-while-over-60-bias-toward-alexa-and-siri/

Kite, M. E., Deaux, K., & Haines, E. L. (2008). Part III: Women's Social and Personality Development. In F. L. Denmark, & B. Lott, *Psychology of Women: A Handbook of Issues and Theories* (pp. 205-332). 06881: Praeger Publishers.

Kvale, S. (1997). *Det kvalitative forskningsintervju.* Oslo: Ad Notam Gyldendal.

Lovdata. (2002, 07 01). Lov om forbrukerkjøp: forbrukerkjøpsloven §4.

Love, D. (2011, Mai 26). *The Shocking Drink And Incredible Coke History Of Subliminal Advertising*. Retrieved from Insider: https://www.businessinsider.com/subliminal-ads-2011-5?r=US&IR=T

Lyon, D. (2003). *Surveillance after September 11.* 65 Bridge Street, Cambridge, UK: Polity Press.
Lyon, D. (2006). *Theorizing Surveillance.* London & New York: Routledge.
Lyon, D. (2007). *Surveillance Studies: An Overview.* Cambridge: Polity Press.
Malkin, N. (2019). *Privacy Attitudes of Smart Speaker Users.* Hentet fra Sciendo: https://doi.org/10.2478/popets-2019-0068
Manikoda, L. D. (2018). *What´s up with Privacy?: User Preferences and Privacy Concerns in Intelligent Personal Assistants*. Hentet fra ResearchGate: 10.1145/3278721.3278773
Marwick, A. E., & Boyd, D. (2014, juli 21). *Networked privacy: How teenagers negotiate context in social media*. Retrieved from Sage : https://doi.org/10.1177%2F1461444814543995
Mathiesen, T. (2013). *Towards a Surveillant Society.* Waterside Press Ltd.
Moon, Y., & Green, N. (2006, Juli 31). *Are Machines Gender Neutral? Gender-Stereotypic Responses to Computers With Voices*. Retrieved from Wiley Online Library: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1559-1816.1997.tb00275.x
Moor, J. H. (1997). *Towards a Theory of Privacy in the Information Age*. Retrieved from Computers and Society: http://www.site.uottawa.ca/~stan/csi2911/moor2.pdf
Nissenbaum, H. (2004). *Privacy as Contextual Integrity*. Retrieved from Washington Law Review: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf
Nissenbaum, H. (2010). *Privacy in Context: Technology, policy and the Integrity of Social Life.* California: Stanford University Press.
NRK. (n.d.). *Hva er en smarthøyttaler?* Retrieved from NRK: https://info.nrk.no/faq/hva-er-en-smarthoyttaler/
Peacock, S. (2014). *How Web tracking changes user agency in the age of Big Data: The used user.* Hentet fra Big Data & Society : https://www.readcube.com/articles/10.1177%2F2053951714564228
Pradhan, A., Findlater, L., & Lazar, A. (2019, November). *"Phantom Friend" or "Just a Box with Information": Personification and Ontological Categorization of Smart Speaker-based Voice Assistants by Older Adults*. Retrieved from ACM: https://doi.org/10.1145/3359316
Press, C. (2018, April 09). *Facebook data: How it was used by Cambridge Analytica*. Retrieved from BBC: https://www.bbc.com/news/av/technology-43674480
Pridmore, J., Zimmer, M., Vitak, J., Mols, A., Trottier, D., Kumar, P., & Yuting, L. (2019, mars 31). *Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households.* Hentet fra Surveillance and Society: https://doi.org/10.24908/ss.v17i1/2.12936
Regjeringen. (2019, Oktober 30). *Ny personopplysningslov*. Retrieved from Regjeringen: https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/
Sagdahl, M. S. (2019, Juni 20). *Verdi*. Retrieved from Store norske leksikon: https://snl.no/verdi
Sagdal, M. S. (2019). *Verdi*. Retrieved from Store norske leksikon: https://snl.no/verdi
Sander, K. (2020, Oktober 29). *Kvalitative intervjumetoder for datainnsamling.* Retrieved from Estudie: https://estudie.no/kvalitative-intervju/
Sander, K. (2020, November 06). *Transkripsjon og transkribering.* Retrieved from Estudie: https://estudie.no/transkripsjon/
Sander, K. (2021, Februar 03). *Kvalitativ metode og design.* Retrieved from Estudie: https://estudie.no/kvalitativ-metode/
Schwär, H., & Moynihan, Q. (2020, April 05). *Companies like Amazon may give devices like Alexa female voices to make them seem 'caring'*. Retrieved from Business Insider:

https://www.businessinsider.com/theres-psychological-reason-why-amazon-gave-alexa-a-female-voice-2018-9?r=US&IR=T
Sommerbakk, J. (2012, Mai 14). «Hvordan håndterer pedagoger i barnehagen barn med reaktiv aggresjonsproblematikk?». *Masteroppgave*. Universitetet i Stavanger.
Taft, J. G. (2019). *The 2nd Synopsium on Application of Contextual Integrity*. Retrieved from Symposium report: https://privaci.info/symposium2/2nd_CI_Symposium_Report.pdf
Tanovska, H. (2020). *Number of digital voice assistants in use worldwide 2019-2023*. Hentet fra Statista: https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/
Thagaard, T. (2003). *Systematikk og innlevelse: En innføring i kvalitativ metode.* Bergen: Fagbokforlaget.
Thornhill, J. (2019, januar 04). *Should we think of Big Tech as Big Brother?* Retrieved from Financial Times: https://www.ft.com/content/43980f9c-0f5b-11e9-a3aa-118c761d2745
Tjora, A. (2017, Januar). *Emergens: Konseptutvikling og generalisering i kvalitativ forskning: Refleksjoner og eksempler*. Retrieved from ResearchGate: 10.13140/RG.2.2.16720.30728
UiB. (2019, Oktober 01). *Krav om registrering av prosjektet ditt i RETTE*. Retrieved from Universitetet i Bergen: https://www.uib.no/personvern/128207/krav-om-registrering-av-prosjektet-ditt-i-rette
Verwijmeren, T., Karremans, J. C., Stroebe, W., & Wigboldus, D. H. (2010, Mai 03). *The workings and limits of subliminal advertising: The role of habits*. Retrieved from ResearchGate: 10.1016/j.jcps.2010.11.004
West, E. (2019, Mars 31). *Amazon: Surveillance as a Service*. Retrieved from Surveillance and Society: https://doi.org/10.24908/ss.v17i1/2.13008
Wolfson, S. (2018, Mai 24). *Amazon's Alexa recorded private conversation and sent it to random contact*. Retrieved from The Guardian: https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation
Woods, H. S. (2018). Asking more of Siri and Alexa: feminine persona in service of surveillance capitalism. *Critical studies in Media Communications*, pp. 334-349.
Østbye, H., Helland, K., Knapskog, K., Larsen, L. O., & Moe, H. (2013). *Metodebok for mediafag.* 5068: Fagbokforlaget.
Øverby, H. (2020, juni 06). *Tingenes internett*. Retrieved from Store norske leksikon: https://snl.no/tingenes_internett
Zuboff, S. (2019). *The Age of Surveillance Capitalism.* London: Profile Books Lft.

Vedlegg

Vedlegg A – Norsk intervjuguide

Intervjuguide norsk

Del 1 (Generelt)

1. Hvor gammel er du?
2. Hva slags smarthøyttaler har du?
3. Hvor ofte bruker du den?
4. Hva bruker du den stort sett til? (Musikk, værmelding, nyheter osv.)
5. Hvor er smarthøyttaleren plassert i hjemmet ditt?
6. Hva ser du på som den beste fordelen med en smarthøyttaler?
7. Hva ser du på som den største ulempen med en smarthøyttaler?
8. Har assistenten din mannlig eller kvinnelig stemme?
9. Var dette et bevisst valg? Hvis ja, hvorfor?

Del 2 (Personvern og overvåking)

1. Hvordan ville du beskrive overvåking? Hva betyr overvåking for deg?
2. Hvordan ville du beskrive personvern? Hva betyr personvern for deg?
3. Hvor viktig er personvern for deg? Er det noe du tenker over når du tar I bruk ny teknologi, eller når du er på internett?
4. Hva anser du som sensitive data? (I forhold til hvilken data teknologiske enheter kan samle inn).

Del 3 (Personvern og smarthøyttalere)

1. En smarthøyttaler har en mikrofon som alltid er på, med mindre du selv skrur av funksjonen. Hva tenker du om det? Har du noen gang skrudd av mikrofonen midlertidig?
2. Har du noen gang mistenkt at assistenten registrerer hva som blir sagt, til tross for at du ikke snakker direkte til den? (F.eks. om du snakker om et produkt du senere får reklame på etc.)
3. Har du noen fått annonser på et produkt du har snakket om, til tross for at du ikke har søkt direkte etter produktet?
4. Alle samtaler mellom deg og assistenten lagres permanent med mindre du skrur av lagringsfunksjonen. Har du noen gang gått tilbake for å høre på disse samtalene?
5. Hvorfor tror du det er en funksjon?
6. Ville det vært for deg om du fikk svar fra en tredjeperson, fremfor Google/Amazon?

Del 4 (Tanker og refleksjoner)

1. Har du noen gang opplevd noe ukomfortabelt I forbindelse med smarthøyttaleren din? (snakker av seg selv osv.) Hvis ja, fortell gjerne.
2. Assistentene har fått kritikk for å være utsatt for hacking. Hva er dine tanker rundt det, er det noe som bekymrer deg?
3. Ansatte fra Google og Amazon lytter til vilkårlige lydopptak fra sine forbrukere. Enten det er fra en henvendelse til assistenten, eller at assistenten har tatt opp lyd ved en feil. Hva er dine tanker rundt det?

Del 5 (Aksept)

1. Hvorfor kjøpte du en smarthøyttaler?
2. Har mange av dine venner en smarthøyttaler?
3. Synes du den er enkel å bruke?
4. Er den til hjelp i hverdagen?

Del 6 (Avsluttende refleksjoner):

1. Stoler du på Amazon/Google til å beskytte ditt personvern?
2. Føler du de har muligheten til å påvirke deg på noen måte?
3. Hvis du har koblet fra smarthøyttaleren: hva skal til for at du kobler den inn igjen?
4. Hvis du har smarthøyttaleren tilkoblet: hva skal til for at du kobler den ut?

Vedlegg B – Engelsk intervjuguide

Interview guide English

Part 1 (General)

1. What is your age?
2. What kind of smart speaker do you have?
3. How often do you use it?
4. What do you mostly use it for? (Music, checking the weather etc..)
5. Where is the smart speaker placed in your home?
6. What do you consider to be the best thing about a smart speaker?
7. Can you tell me what you consider to be the most negative thing about a smart speaker?
8. Does your assistant have a male or female voice?
9. Did you choose to have a male of female voice, or was that preset?

Part 2 (Privacy and surveillance)

1. What does the term surveillance mean to you, how would you describe the term?
2. What does the term privacy mean to you, and how would you describe the term?
3. How important is privacy to you, is that something you take into consideration when implementing new technologies into your life, or when you are creating an online account, or when you share things on social media?
4. In regards to technology devices, what do you consider to be sensitive data? (photos, voice recordings, private videos from inside the home, text, identification information etc.)

Part 3 (Privacy and smart speakers)

1. A smart speaker has a microphone that is always on, unless you mute the speaker or turn it off. What are your thoughts on that, have you ever turned the microphone off temporarily?
2. Have you ever suspected that the smart speaker have listening to you conversation, even though you have not said its trigger word?
7. Have you ever received ads after a conversation, even though you did not actively search for that product online?
8. Every conversation between you and your smart speaker are stored permanently unless you change the setting, and can be listened to afterwards. Have you ever done that?
9. Why do you think that is a function?
10. Would you have an issue with a third party answering your question?

Part 4 (Thoughts and reflections)

4. Have you experienced a situation with you smart speaker that was uncomfortable? (talking on its own etc..) If so, please share.
5. Studies have shown that its quite easy to hack peoples smart speakers. Is that something that worries you, or something you have taken into consideration?
6. Employees from Google and Amazon listens to random recordings from users, whether that is an intentional interaction, when the speaker records by a mistake. What are your thoughts on that, are you comfortable with that?

Part 5 (Accept)

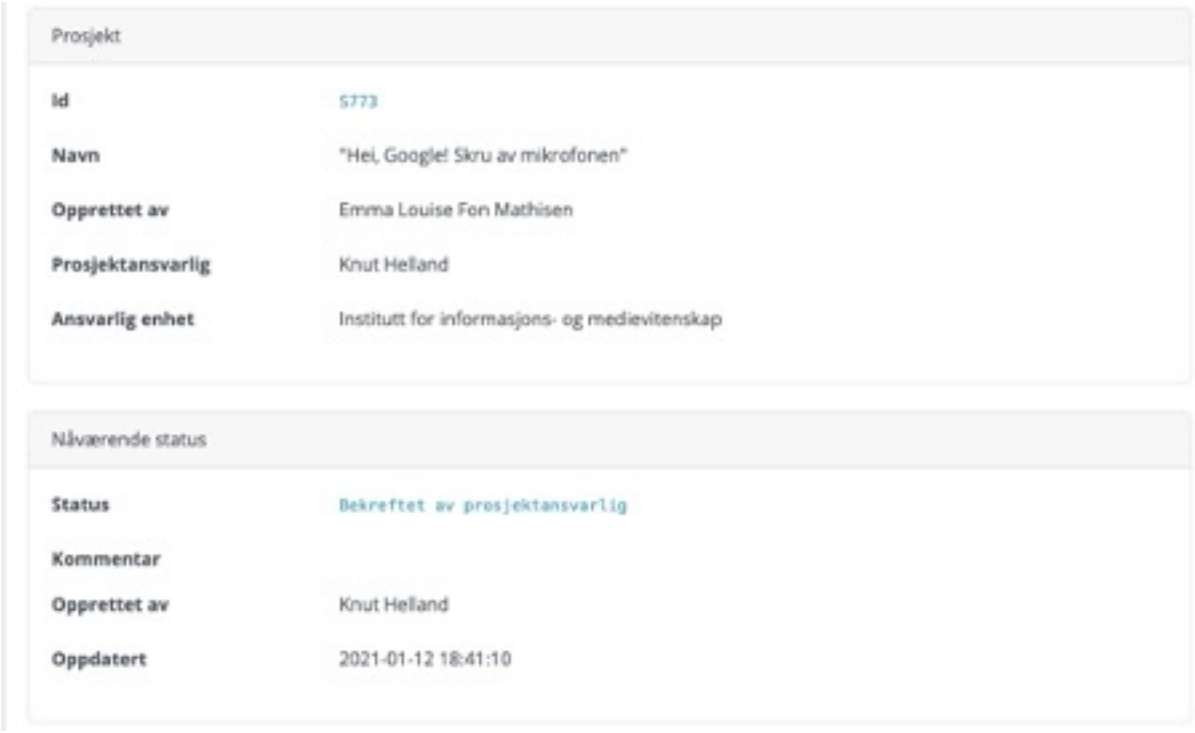
5. What made you buy a smart speaker? (A friend, an ad, curiosity etc..)
6. Does a lot of your friends have a smart speaker?
7. Do you find it easy to use?
8. Do you find it helpful in everyday tasks?

Final thoughts:

1. Do you trust Amazon and Google to protect your privacy?
2. Do you feel they have the power to influence you in any way? (targeted ads etc..)
3. If you have disconnected the speaker: what would it take for you in order to reconnect the speaker?
4. If you have the speaker connected, what would be a reason for you to disconnect the speaker?

Vedlegg C – Godkjennelse Rette

Prosjektets ID på RETTE: **S773**



Prosjekt

Id	S773
Navn	"Hei, Google! Skru av mikrofonen"
Opprettet av	Emma Louise Fon Mathisen
Prosjektansvarlig	Knut Helland
Ansvarlig enhet	Institutt for informasjons- og medievitenskap

Nåværende status

Status	Bekreftet av prosjektansvarlig
Kommentar	
Opprettet av	Knut Helland
Oppdatert	2021-01-12 18:41:10