Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for økonomi
Institutt for industriell økonomi og teknologiledelse

Marianne Aas Karlsen

Personvernparadokset

En kvalitativ studie om bruk av smartklokker

Bacheloroppgave i Økonomi, ledelse og bærekraft
Veileder: Aristidis Kaloudis
Mai 2022

NTNU
Kunnskap for en bedre verden

Marianne Aas Karlsen

Personvernparadokset

En kvalitativ studie om bruk av smartklokker

Bacheloroppgave i Økonomi, ledelse og bærekraft
Veileder: Aristidis Kaloudis
Mai 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for økonomi
Institutt for industriell økonomi og teknologiledelse

NTNU
Kunnskap for en bedre verden

Forord

I dag er det min innleveringsdag for bacheloroppgaven. Jeg kan nå se tilbake på en periode med annerledes studiearbeid, noe som både har gitt frustrasjon, men også mestringsfølelse.

Jeg har hatt flere bidragsytere underveis som jeg må takke for at jeg har kommet i mål! Først og fremst må jeg takke den nære familien for støtte og oppmuntring gjennom studieårene. Gjennom bacheloroppgaven må jeg gi en spesiell takk til Ketil som står støtt ved siden av og er en god diskusjonspartner, samt Ida som har bidratt med gjennomgang av det engelske abstraktet.

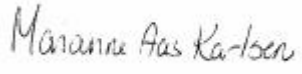
En takk fortjener også kollegaer som har stilt opp på intervjuer og gitt meg verdifull bakgrunnsinformasjon, men også Team Anfield for deres tålmodighet gjennom det siste semesteret.

Sist, men ikke minst, en takk til min veileder, Aristidis Kaloudis. Han har stått ved siden av med råd og veiledning under arbeidet med oppgaven. Hele veien har han vist interesse, vært proaktiv i forhold til veiledningsmøter, samt at det aldri er vanskelig å få han i tale.

En felles takk til dere alle for å ha gitt meg følelsen av at dere ønsker jeg skal lykkes med oppgaven!

Askim, 19. mai 2022

Marianne Aas Karlsen



Sammendrag

Tittel:	Personvernparadokset – En kvalitativ studie om bruk av smartklokker	Dato: 190522
Deltaker:	Marianne Aas Karlsen	
Veileder:	Aristidis Kaloudis	
Stikkord/ nøkkelord (3-5 stk)	Personvernparadokset, Personvern, Smartklokke, Helseopplysninger.	
Antall sider/ord: 50 sider / 16.311 ord	Antall vedlegg: 8	Publiseringsavtale inngått: Ja

Flere og flere tar i bruk smartklokker og for mange er smartklokker et nyttig og motiverende hjelpemiddel for å holde seg i form og bidra positivt til egen helse. Samtidig genererer smartklokkene mye data, noe som tilsier at smartklokkeprodusentene høster stort volum av persondata og hvor deler av disse er å anse som helseopplysninger.

Formålet med studien er å forstå hvilke vurderinger smartklokkebrukere gjør i forhold til bruksverdien av de sensitive persondata som smartklokker genererer. Gjennom oppgaven blir man kjent med begrepet personvernparadokset som forklarer gapet mellom den bekymring vi har om informasjon vi deler om oss selv og ønsket om et sterkt personvern slik at våre data ikke kan misbrukes. I kombinasjon med personvernparadokset legges det til grunn følgende tre teorier; teorien om planlagt atferd, teorien om rasjonell uvitenhet og teorien om beskyttende motivasjon.

Seks informanter ble intervjuet ved hjelp av en semistrukturell intervjuguide. Ikke overraskende bryr informantene seg lite om brukervilkår og personvernerklæringer. Derimot er de bevisste på å styre tilgang til data gjennom aktive valg av innstillinger i smartklokkenes digitale grensesnitt. Det som var overraskende i studien, var en utbredt «*jeg har intet å skjule*»-holdning. Ingen av informantene klarte å komme på utfordrende scenarioer som indikerer hvordan deres helseopplysninger kunne bli misbrukt.

Studien gir et tydelig uttrykk for at informantene ikke er bekymret for helseopplysninger som ens smartklokke genererer. Ei heller forventer de at helseopplysningene har noen bruksverdi for andre aktører. Konklusjonen er at det ikke eksisterer noen personvern-paradoks i denne studien.

Abstract

Title:	Privacy Paradox – A qualitative study about smartwatches	Date: 190522
Participant:	Marianne Aas Karlsen	
Supervisor:	Aristidis Kaloudis	
Keywords (3-5 words)	Privacy paradox, Privacy awareness, Smartwatch, Health information.	
Number of pages/words: 50 pages / 16.311 words	Number of appendixes: 8	Availability: Open

The number of people using smartwatches is rapidly increasing. Smartwatches can be a useful tool in motivating us to stay in shape, and hence contribute positively to our health. Nevertheless, smartwatches generate a lot of data, which enables manufacturers to harvest a large amount of personal data, including sensitive health information.

This thesis studies smartwatch users and their understanding regarding the value of the sensitive personal information that their smartwatches generate. Through this thesis, one becomes familiar with the concept of the privacy paradox, which describes the gap between our concerns regarding privacy and our behavior to share information online. In combination with the privacy paradox, the following three theories will lay the groundwork for the thesis; theory of planned behavior, theory of rational ignorance, and the protective motivation theory.

Through a qualitative study, six informants were interviewed in the form of a semi-structured interview. As expected, the informants did not care much about the terms of use and the privacy statement when it comes to the use of smartwatches. On the other hand, they are very conscious of restricting access to data using available user settings. Surprisingly, there was a widespread «*I have nothing to hide*»-attitude. This attitude further led to no one being able to come up with any particularly challenging scenario on how their sensitive health information could be misused.

None of the informants feels worried about the health information that one's smartwatch generates and do not expect the health information to have any value for other companies. Conclusion; there is no existence of privacy paradox in this thesis.

Innholdsfortegnelse

Oversikt over figurer

Oversikt over tabeller

1. Innledning

Gjennom siste del av studieløpet har jeg vært interessert i å lære mer om kunstig intelligens og digital etikk, men tiden har ikke strukket til på grunn av kombinasjon fulltidsjobb og studier. Endelig kom tiden for å jobbe med bacheloroppgaven med mulighet til å studere selvvalgt tema. Jeg har lest mye og bredt om kunstig intelligens og digital etikk som en forberedelse, selv om få av disse kildene refereres i oppgaven. Etter hvert har jeg avgrenset mitt interessefelt til å omfatte tanker og holdninger rundt bruk av sensitive data, og da er smartklokkene en relevant case for en empirisk studie av brukernes tanker om bruksverdien av data som generes av smartklokkene deres.

I helsesektoren er man nødt til å håndtere innbyggernes helseopplysninger innenfor et sikkert internett som forvaltes og driftes av Norsk helsenett (Norsk helsenett, 2022). For de virksomheter som tilkobler seg Norsk helsenett stilles det krav om å følge Normen (Direktoratet for e-helse sin norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Direktoratet for e-helse, 2020)). På denne måten er våre helseopplysninger sikret i vår samhandling med helsevesenet. Når det gjelder bruk av dagens smartklokker, vil de også generere sensitive helseopplysninger som f.eks. puls- og søvnverdier. Helse-opplysningene som genereres av smartklokker har derimot ikke samme datasikkerhetsnivå som øvrige helseopplysninger. De er tilgjengelig gjennom det ordinære internettet og hvor vi ikke bare synkroniserer data mellom smartklokke og smartklokkeprodusent, men også videre til 3. parter. Synkroniseringen muliggjør samhandling med andre smartklokkebrukere og hvor det bidrar til både nytte og motivasjon.

Som en følge av at jeg jobber med kunder innenfor helsesektoren, har mine kollegaer og jeg et bevisst forhold til at helseopplysninger er å anse som sensitive og skal skjermes, noe som også følges av lov om personopplysninger (Lovdata, 2018a). Derimot er det slik at vi som privatpersoner stadig deler mer informasjon om oss selv med de som er oss nære, men også til utenforstående all den tid man deler informasjonen på internett. Det er ikke alle som har et bevisst forhold til at man faktisk deler informasjon med utenforstående på internett. De fleste av oss har likevel en naturlig, iboende tanke og en forståelse om at den informasjonen vi deler, kun blir tatt imot på en god måte av de man har definert en relasjon med.

1.1 Formål og problemstilling

Det blir bare flere og flere av oss som benytter smartklokker. Samtidig blir klokkene også smartere og tilgjengelig funksjonalitet er gjennom kontinuerlig utvikling. Som en følge av dette, måler vi stadig flere parametere, både for egen del, men også for andre da det gir oss mulighet for sammenligning. Målinger kan spore til motivasjon og er kanskje hovedgrunnen til at mange anskaffer seg en slik smartklokke. Samtidig, er det greit at man synkroniserer data både til smartklokkeprodusent og 3. parts aktører? Bruker man smartklokken som en del av aktivitet eller søvn, vil de data som smartklokken genererer være definert som helse-opplysninger og av den grunn ansett som sensitive. Hvordan blir disse helseopplysningene håndtert av smartklokkeprodusentene? De vil ha et ønske om å benytte kundenes data til produktforbedringer med formål om å øke sine markedsandeler. Parallelt sitter de på et stadig voksende datavolum av sensitive data. Det er en forventning at smartklokkeprodusentene oppfyller dagens GDPR-krav (EU, 2016) og dermed behandler disse dataene med varsomhet og etter regelverket. Samtidig, hver av oss er bare én i mengden og blir dermed som enkeltindivider et nyttig redskap for å skape store datavolum. Smartklokkeprodusenter kan benytte analytiske verktøy som kunstig intelligens og Big Data for å finne mønstre vi som enkeltpersoner ikke har stor nok fantasi om – uten å bli betegnet som en skeptiker. Gjennomføres innsamlingen og behandlingen av personopplysninger fra smartklokke-produsentenes side på en forsvarlig måte? Og har produsentene nødvendig kunnskap, datainfrastruktur og integritet som trengs til en forsvarlig og etisk behandling av sensitive data som smartklokkebrukere produserer og deler? Bacheloroppgaven har som formål å utforske sider ved disse spørsmålene. Forhåpentligvis kan oppgaven bidra til å øke vår bevissthet knyttet til verdien av våre sensitive helseopplysninger og hvordan de på sikt muligens kan få andre bruksområder. Dette bringer oss til oppgavens problemstilling:

> ***Hvilke vurderinger gjør smartklokkebrukere om bruksverdien til de sensitive persondata som ens smartklokke genererer?***

Gjennom litteratursøk i oppstartsfasen har jeg identifisert et relevant teoretisk begrep, nemlig «Personvernparadokset». Personvernparadokset forklarer avviket mellom våre holdninger til personvern på internett kontra vår faktiske atferd innenfor bruk av internett. Utforskning av personvernparadokset som et sosialt fenomen er den røde tråden som følger oppgaven.

1.2 Avgrensning og begrepsavklaringer

Bacheloroppgaven er avgrenset til å omhandle data som smartklokker genererer som følge av brukerens aktivitet og søvn. En smartklokke innehar ofte flere funksjoner og hvor tilgjengelige muligheter vil avhenge av både smartklokkeprodusent og -type, dog vil disse dataene ikke bli utforsket nærmere.

Personopplysninger – «*Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson.»* (Datatilsynet, 2019).

Helseopplysninger – en gruppering av personopplysninger som er særs skjermet i personopplysningsloven. All behandling av personopplysninger i en slik kategori og hvor formålet er å identifisere en fysisk person, er forbudt. For å behandle helseopplysninger om deg som enkeltperson, er aktøren avhengig av et samtykke fra deg (Lovdata, 2018a).

Smartklokke – klokke som har tilleggsfunksjoner utover det å være en ordinær klokke og som kan synkroniseres med andre enheter. Imidlertid finnes en glidende overgang mellom smartklokker og sportsklokker. I denne oppgaven dekker begrepet smartklokke begge typer klokker.

Bruker – en person som bruker en smartklokke aktivt i hverdagen og som synkroniserer data med andre enheter.

Brukerkonto – består av et brukernavn, passord og annen informasjon som er relatert til brukeren. Ved hjelp av brukerkonto og passord kan brukeren logge inn på ett system, som for eksempel en app eller en webside.

Aktør – en virksomhet som mottar smartklokkedata fra brukere og som gir brukerne tjenester i retur i form av brukergrensesnitt for å følge både egne og andres aktivitet. Avhengig av brukernes samtykke, kan aktørene benytte smartklokkedataene til andre formål, som f.eks. forskning og markedsaktiviteter.

Personvernparadoks – et avvik mellom våre holdninger til personvern på internett kontra vår faktiske atferd innenfor bruk av internett.

Strava – en digital treningsapp.

Big Data – også kalt stordata og «*…er et begrep som refererer til datamengder som er så store at de ikke lar seg gjennomgå av vanlig programvare*.» (Bergsjø og Bergsjø, 2019).

1.3 Videre struktur i oppgaven

I neste kapittel viser jeg til relevant teori som blir benyttet for å besvare problemstillingen. Kapittel 3 drøfter valg av metode som studien er basert på. Kapittel 4 presenterer de empiriske funnene fra studiet, mens kapittel 5 drøfter funnene sett opp mot valgte teorier og problemstilling. Siste kapittelet gir oss konklusjonen, samt beskriver muligheter for videre forskningsarbeid.

2. Teoretisk grunnlag og begrepet «personvernparadokset»

Dette kapittelet redegjør først for historien til begrepet personvernparadokset. Deretter går jeg videre til relatert forskning og fokuserer først på en litteraturstudie basert på personvern-paradokset opp mot beslutningsteorier. Videre beskrives to svært relevante studier knyttet til smartklokker. Den ene tar opp igjen personvernparadokset og kobler dette med smartklokker, mens det andre studiet går på personvernets bevissthet og smartklokkebrukerenes atferd. Deretter presenteres jeg teoriene som bacheloroppgaven legger til grunn og til sist kommer en gjennomgang av de forventede funn i studien.

2.1 Personvernparadokset

Personvernparadokset er et begrep som forklarer gapet mellom den informasjon vi deler om oss selv på internett og hvor vi parallelt ønsker oss et sterkt personvern som sikrer at våre data ikke misbrukes. Om resultatet blir et personvernparadoks for den enkelte, avhenger av hvilke valg den enkelte tar. Hverdagen består av mengder av valg, både små og store, samt at noen valg er mer bevisste enn andre. Men hvorfor havner man i situasjoner som kan betegnes som personvernparadoks?

2.1.1 Personvernsparadoksets historie og bakgrunn

Ifølge flere kilder, Norton (Norton, 2021), The Privacy Issue (Ker, 2020) og The Extended Mind (Carbonneau, 2021) opplyses det at begrepet «*The Privacy Paradox*» først ble benyttet av forskeren Barry Brown hos Hewlett Packard. Brown forsket blant annet på netthandel og avdekket i den forbindelse brukernes bekymringer knyttet til personvern og opp mot supermarkedenes lojalitetsprogram (Brown, 2001). Brown benyttet begrepet «privacy paradox» i anførselstegn. I senere tid har begrepet blitt innarbeidet og står godt alene, uten anførselstegn.

Videre benyttet Barnes begrepet i 2006 når hun forsket på personvernutfordringer og de unges bruk av sosiale nettverk (Barnes, 2006). I tillegg benyttet Norberg, Horne og Horne også begrepet i 2007 hvor de undersøkte selve personvernparadokset ved å ha fokus på hva man avgir av personlig informasjon kontra hva som avsløres om ens reelle atferd (Norberg, Horne og Horne, 2007).

Samtidig hevdet Solove at det var Norberg, Horne og Horne som hadde opprinnelsen til begrepet personvernparadokset i deres artikkel fra 2007 og at det var fra denne tiden begrepet ble «offisielt» og et fenomen stadig flere refererer til (Solove, 2021). Solove argumenterte

også for at personvernparadokset var en myte som ble skapt av en logisk brist. Han hevdet at studier om personvernparadokset og menneskers beslutninger om risiko var knyttet til veldig konkrete og spesielle sammenhenger, mens holdningen til personvernet var mer generelt. Han mente derfor det ble feil å generalisere beslutninger rundt spesifikke personopplysninger i spesifikke sammenhenger opp mot hvordan mennesker generelt verdsetter privatlivet sitt. Videre trodde ikke Solove at løsningen for paradokset var å gi enkeltpersoner ytterligere muligheter og individuelle valg til selv å regulere bruk av egne data. Han betraktning var: «*Administrasjon av ens regelverk er et stort, komplekst og et uendelig prosjekt som ikke skalerer og som er tilnærmet umulig å gjennomføre helhetlig*» (Solove, 2021). Solove mente vi heller burde sette søkelys på å regulere arkitekturen og struktur rundt bruk, vedlikehold og overføring av data på et systemisk nivå.

2.2 Relatert forskning på personvernparadokset

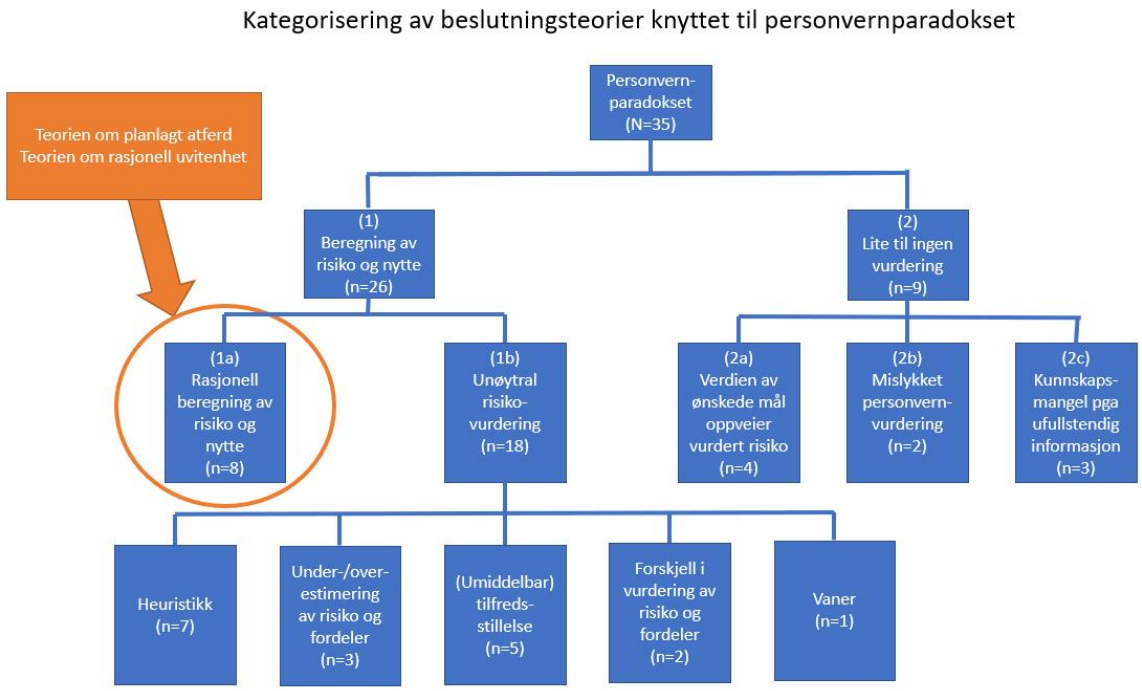
For å finne litteratur innenfor temaet har jeg søkt i bibliografiske databaser som NTNU Universitetsbibliotek og Web of Science. Jeg har blant annet benyttet søkeordene «privacy awareness», «privacy paradox», «privacy concerns», «smartwatch» og «health information», men også aktivt benyttet forskjellige studiers referanser for å finne relatert litteratur. På bakgrunn av dette arbeidet, har jeg valgt å sette søkelyset på tre relevante kilder for denne oppgaven. Nedenfor gis en mer detaljert presentasjon av det teoretiske grunnlaget som publikasjonene identifiserer.

2.2.1 Barth og de Jong – Personvernparadokset og beslutningsteorier

Basert på et ønske om å forklare personvernparadokset gjennomførte Barth og de Jong en systematisk litteraturstudie knyttet til hvilke beslutningsteorier som kan forklare personvern-paradoksets tilstedeværelse på internett (Barth og de Jong, 2017). De startet med å søke opp «privacy paradox» i forskningsdatabaser og hvor de plukket ut forskjellige studiene basert på relevans. Relevansen ble kryssjekket manuelt opp mot referanselister for å fange opp studier som ikke dukket opp under første søk. Deretter ble disse studiene analysert i forhold til om teoriene diskuterte personvernparadokset. Etter nødvendig siling av studier, endte forskerne opp med 32 studier hvor 35 ulike teorier innenfor beslutningsteori ble lansert og drøftet.

Teoriene ble kategorisert i gruppene rasjonelle og irrasjonelle tilnærminger til personvern-paradokset og hvor flertallet av teoriene fokuserte på forholdet mellom risiko og nytte. Det viste seg at nytten, og dermed fordelene, oppveide risiko og eventuelle ulemper.

Kategoriseringen av beslutningsteoriene er vist i figuren under og hvor disse teoriene kan bidra til å forklare personvernparadokset:



Figur 2.1: Kategorisering av teorier knyttet til personvernparadokset og beslutningstaking. Modellen til Barth og de Jong er oversatt og modifisert for oppgavens behov (Barth og de Jong, 2017)

I kategoriseringen dannet det seg to hovedgrupper, hvorav den første gruppen (1) omhandlet rasjonell beregning av risiko og nytte, mens den andre gruppen (2) gjorde liten eller ingen risikovurdering og hvor det handlet mest om bruksfordeler.

Den første hovedgruppen kunne igjen deles i to undergrupper. Den første undergruppen (1a) var i hovedtrekk rasjonelle i forhold til risiko, men parallelt overstyrte fordelene den risiko som fantes. Den andre undergruppen (1b) var derimot ikke nøytrale i sin risikovurdering og hvor det handlet mest om de fordeler man oppnådde. Denne undergruppen ble videre delt inn fem forskjellige skjevheter som påvirket beslutningsprosessen:

- Heuristikk – Vi tar i bruk mentale snarveier som i stor grad favoriserer fordelene.
- Under-/overvurdering av risiko og fordeler – Vi undervurderer vår egen risiko i forhold til personvernet, mens vi parallelt overvurderer andres risiko for at de opplever uønskede hendelser (det skjer de andre – ikke meg). Når det gjelder medias effekt, undervurderer vi effekten media har på oss selv, mens vi

overvurderer effekten på andre (jeg lar meg ikke påvirke av media – det gjør de andre).

- Umiddelbar tilfredsstillelse – Vi mangler selvkontroll fordi vi søker umiddelbar tilfredsstillelse i stedet for å vurdere om det kan være negativt på lengre sikt.
- Forskjell i vurdering av risiko og fordeler – Vår vurdering av personvern og dens trusler eller risiko føles ofte abstrakt, mens datatjenester gir oss konkrete fordeler. Konkrete fordeler kan derfor ofte veie opp for abstrakte trusler eller risiko.
- Vaner – Vi har lært oss enkelte rutiner som gjør at vår atferd går på automatikk.

Den andre hovedgruppen, som gjorde liten eller ingen vurdering, var også delt i undergrupper. Den første undergruppen (2a) omhandlet verdien av at et ønsket mål oppveide den vurderte risikoen. Den andre undergruppen (2b) handlet om at en mislykkes i å gjøre en personvernvurdering og hvor den tredje (2c) skyldtes kunnskapsmangel som følge av at man har for liten informasjon å basere beslutningen på.

Barth og de Jong hadde som mål for litteraturstudiet at de skulle forklare personvern-paradokset gjennom beslutningsteorier. Forskerparet konkluderte med at de foretrakk å benytte en kombinasjon mellom rasjonell og irrasjonell beslutningstaking for å redusere personvernparadokset. Samtidig mente de at det burde være god design på løsninger, slik at brukerne selv på en enkel måte sørget for økt beskyttelse av egne data.

Gjennom studiet har Barth og de Jong gitt oss en oversikt over litteraturen innenfor personvernparadokset og beslutningsteorier. Gjennom analysen jeg gjorde av informantene opp mot de 35 ulike beslutningsteoriene, besluttet jeg å benytte 2 av beslutningsteoriene, teorien om *planlagt atferd* og *rasjonell uvitenhet* (se markering i figur 2.1).

I etterkant av studien til Barth og de Jong har det blitt utført en annen studie av personvern-paradokset og som var knyttet konkret opp mot bruk av smartklokker.

2.2.2 Williams, Nurse og Creese – Personvernparadokset og smartklokkespill

Williams, Nurse og Creese forsket også på personvernparadokset og hvor de mente dette var utbredt på smartklokker (Williams, Nurse og Creese, 2019). Fra tidligere arbeid var det blitt foreslått at manglende oppmerksomhet rundt personvernparadokset kan løses gjennom å øke

oppmerksomheten. Målet til William, Nurse og Creese ble derfor å bidra til redusering av personvernparadokset og hvor de utviklet et smartklokkespill for å øke smartklokkebrukernes kunnskap. For å kontrollere resultatet i etterkant, ble deltakerne delt inn i en behandlings-gruppe og en kontrollgruppe. Behandlingsgruppen fikk skreddersydd smartklokkespillet til personvern, mens kontrollgruppen fikk samme spill – men ikke tilsvarende tilpasning.

Gjennom studiet vurderte forskerne flere teorier. Av beslutningsteoriene som også Barth og de Jong var innom, var teoriene om *begrunnet handling* (Theory of Reasoned Action) og *planlagt atferd* (Theory of Planned Behavior). Imidlertid mente Williams, Nurse og Creese at disse to teoriene ikke passet for deres oppdrag og landet på bruk av teorien for *beskyttende motivasjon* (Protection Motivation Theory) fordi teorien stemte godt overens med personvern. De henviste også til at Briggs et al. anbefalte bruk av denne teorien for endring av sikkerhetsatferd (Williams, Nurse og Creese, 2019). Teorien om *beskyttende motivasjon* søker å forklare hvorfor/hvorfor ikke individene søker å beskytte seg. Gjennom funnene og videre drøfting konkluderte de med at det var trusselskomponentene som var de største og innflytelsesrike faktorene.

Det viste seg at brukerne selv hadde et balansert syn i forhold til alvorlighetsgraden. Hadde de samtykket til nødvendige tilganger og derved fått belønningen for å komme i gang med smartklokken – var brukerne fornøyd. Samtidig oppfattet ikke kontrollgruppen noen risiko gjennom prosessen og hvor forskerne mente det skyldes at denne gruppen ikke hadde fått opplæringen i dataenes verdi. Det var først etter at brukerne hadde spilt smartklokkespillet med personverntilpasningen at de reflekterte over hva slags tilgang de ga til egne data. Videre var det en grunn til at smartklokkene ble anskaffet og skal man begrense tilganger innebærer det parallelt at fordelene reduseres. Av den grunn vil den informerte bruker kun dele visse typer data, mens andre typer data aktivt beskyttes. Studiet til Williams, Nurse og Creese beviste at smartklokkespill kan bidra til å øke vår bevissthet i forhold til personvern og bruk av smartklokker.

2.2.3 Udoh og Alkharashi – Bevissthet om personvernrisiko og smartklokkebrukernes atferd

Udoh og Alkharashi gjennomførte også en studie opp mot smartklokker. De hadde ikke fokus på selve begrepet personvernparadokset, men temaet lå likevel nærme all den tid de fokuserte på smartklokkebrukernes holdning og bevissthet til personvern og hvordan disse faktorene spilte inn på deres atferd ved bruk av smartklokker (Udoh og Alkharashi, 2016). Deres

konferansepaper har flere elementer som samsvarer med denne bacheloroppgaven, samt at Williams, Nurse og Creese sitt ovenstående studie også refererte hit (Williams, Nurse og Creese, 2019).

Deres studie hadde ikke flere enn 10 deltakere og hvor de påpekte denne begrensningen. Til tross for dette, meldte de om interessante funn. Et av funnene var at bruken av smartklokkene var noe begrenset i forhold til de muligheter en smartklokke faktisk kan gi. I hovedtrekk ble smartklokken brukt for å overvåke helsen, logging av trening og veibeskrivelser. Et annet funn var at det var identitetstyveri som toppet listen over personvernbekymringer, mens både helseopplysninger og GPS-data ble rangert lavere. En mulig grunn til rangeringen mente de skyldes at informantene var i alderen 19-26 år og hvor disse har et nærere forhold til sosiale medier enn mange andre aldersgrupper. Videre fant de at bekymringer rundt personvernet korrelerte med ens holdning til personvern generelt. På bakgrunn av aldersgruppen, var det ikke overraskende at det var en stor andel som uttrykte en «*jeg har intet å skjule*»-holdning. Samtidig argumenterte informantene med at det er forskjellige nivåer av sensitivitet knyttet til de data som en smartklokke genererer og lagrer. Imidlertid mente de at deling av personlige rekorder ville gi inspirasjon til andre. Udoh og Alkharashi fant også ut at kulturell bakgrunn påvirket holdningen til personvern. Det viste seg at de nordamerikanske informantene var mer forsiktig med personvernet enn de andre deltakerne. På slutten av intervjuene erfarte forskerne en holdningsendring som følge av bevisstgjøring og at risiko ble påpekt.

Udoh og Alkharashi konkluderte med at argumentet informantene hadde i starten av intervjuet, «*jeg har intet å skjule*», endret seg noe frem mot slutten av intervjuene og hvor informantene innrømmet at de også hadde behov for et privatliv. Samtidig hadde de ingen forklaring på manglende personvernforberedelser knyttet til bruken av smartklokken, annet enn at de ikke forventet noen brudd på personvernet. I stedet var de mer opptatt av å sikre smarttelefonen sin enn smartklokken.

Etter avsluttet studie, mente Udoh og Alkharashi at de hadde gitt nye perspektiver til kompleksiteten rundt personvern og sikkerhet ved bruk av smartklokker, samt vist at kompleksiteten var mer utfordrende enn forventet.

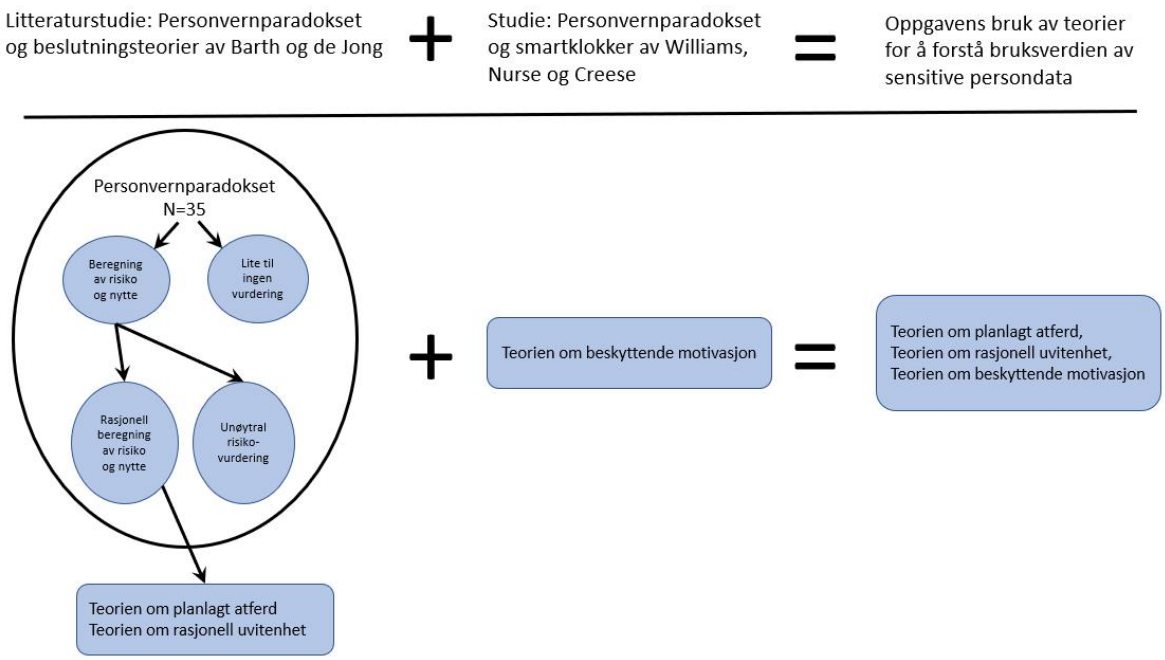
2.3 Det teoretiske perspektivet

For å finne frem til oppgavens relevante beslutningsteorier fra litteraturstudien til Barth og de Jong (Barth og de Jong, 2017), studerte jeg informantenes tilbakemeldinger og analyserte de opp mot de 35 ulike beslutningsteoriene. Med et utgangspunkt i teoriens navn og hvor de var

kategorisert i hierarkiet til personvernparadokset, som vises i figur 2.1, fikk jeg redusert antall mulige relevante teorier ned til 26 ulike beslutningsteorier. For å redusere ytterligere antall teorier, satte jeg meg inn i de overordnede beskrivelsene for hver av de 26 beslutningsteoriene som lå i litteraturstudiets appendiks for å vurdere relevansen. Resultatet ble 16 mulige relevante teorier som var spredt i hierarkiet. For ytterligere reduksjon, ble disse 16 teoriene satt opp i et Excel-ark. Igjen, basert på litteraturstudiets overordnede teoribeskrivelser, ble hver tilbakemelding på hvert spørsmål for den enkelte informant vurdert og koblet til relevant teori. Med tanke på antall treff fra informantene, var det 3 beslutningsteorier som pekte seg ut, teorien om *rasjonell uvitenhet, rasjonelle valg* og *planlagt atferd.* Alle 3 beslutningsteorier var kategorisert i undergruppen for *Rasjonell beregning av risiko og nytte (1a)* (ref. figur 2.1).

For å ha en mulighet til å kontrollere om resultatet var korrekt, gjennomførte jeg en overordnet kobling opp mot den enkelte informant. Da studerte jeg de enkelte tilbakemeldingene, som allerede var koblet opp mot teorier, og kombinerte disse resultatene med tilhørende refleksjonsnotat fra aktuelt intervju. Resultatet ble tilnærmet det samme, dog med unntak av at jeg ikke klarte å koble noen av informantene overordnet opp mot teorien om *rasjonelle valg.*

På bakgrunn av antall treff på beslutningsteorier i kontrollen og som blir drøftet i kapittel 5.6, besluttet jeg å gå videre med 2 beslutningsteorier fra litteraturstudien til Barth og de Jong (Barth og de Jong, 2017); teorien om *planlagt atferd* og *rasjonell uvitenhet*. I tillegg til de valgte beslutningsteoriene, vil jeg også benytte teorien fra studiet til Williams, Nurse og Creese (Williams, Nurse og Creese, 2019), nemlig teorien om *beskyttende motivasjon.* Bakgrunnen for at jeg velger å inkludere denne teorien, skyldes relevansen mellom våre studier. Til sammen utgjør dette mitt teoretiske fundament for oppgaven. I figuren under vises beslutningsveien for valg av teorier:

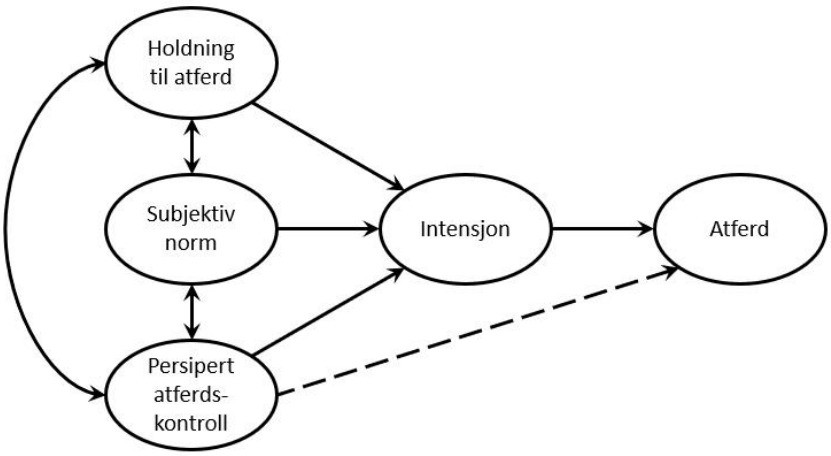


Figur 2.2: Beslutningsvei for bruk av teorier i bacheloroppgaven

2.3.1 Theory of Planned Behavior (TPB) – Planlagt atferd

Teorien om *planlagt atferd* er utviklet for både å forutsi og forklare menneskelig atferd i konkrete situasjoner. Ajzen videreutviklet teorien på bakgrunn av hans og Fishbeins arbeid med teorien for *begrunnet handling* (Theory of Reasoned Action – TRA). Selve teorien om *begrunnet handling* viser til at et individs atferdsmessige intensjon både er avhengige av dens holdning til en spesifikk atferd og subjektive normer som enkeltindividet erfarer. Begge deler knyttes til den aktuelle atferden gjennom intensjonen om en spesifikk atferd. Forskjellen mellom teoriene *begrunnet handling* og *planlagt atferd*, skyldes elementet som omhandler opplevd atferdskontroll. Gjennom dette elementet er det økt mulighet for å forutsi menneskelig atferd (Ajzen, 1991).

Teorien kan beskrives gjennom følgende modell:



Figur 2.3: Teori for planlagt atferd. Modellen til Ajzen er oversatt og modifisert for oppgavens behov (Ajzen, 1991)

Teorien om *planlagt atferd* gir oss tre uavhengige komponenter som knyttes til intensjon:

1. Holdning til atferd – beskriver den oppfatning eller innstilling et individ har til en bestemt handling eller atferd. Intensjonen og senere atferden påvirkes av om holdningen er positiv eller negativ.
2. Subjektiv norm – den sosiale faktoren som sier noe om hvilket press som oppfattes fra omgivelsene og hvordan det påvirker ens intensjon om en konkret atferd.
3. Persipert atferdskontroll – forteller om graden av ens oppfattet adferdskontroll. Refleksjon fra tidligere erfaringer vil påvirke forventningen om eventuelle utfordringer.

Alle komponentene gir uavhengige bidrag til intensjon og atferd. På den måten vil kun én av komponentene alene påvirke intensjonen og dertil atferden. Andre ganger vil det være en kombinasjon av komponentene som påvirker.

I følge Ajzen finnes en generell regel om at jo mer positiv en holdning og en subjektiv norm er – i forhold til en spesifikk type atferd – jo bedre følelse har man for den persiperte atferdskontrollen. I kombinasjon vil dette oppmuntre et individs intensjon om å vurdere sin atferd (Ajzen, 1991). Regelen tilsier at jo sterkere en engasjerer seg i en spesifikk atferd, jo mer sannsynlig er det at man får betalt for den innsatsen man nedlegger. Det som imidlertid er viktig, er at man har autonomi. I tillegg vil det være behov for at man både har muligheter og ressurser tilgjengelig, slik som penger, tid, ferdigheter og eventuelt mulighet for samarbeid. I sum kan dette bidra til at det enkelte individ gis mulighet til å oppnå en faktisk kontroll over egen atferd. Har man motivasjon i tillegg, har man gode sjanser til å lykkes med konkrete mål.

Om man derimot opplever at man ikke har nødvendig kontroll, vil oppfattelsen påvirke vår intensjon og dertil handlinger. Det kan bety at man ikke har nødvendige forutsetninger for å utøve en ønsket atferd.

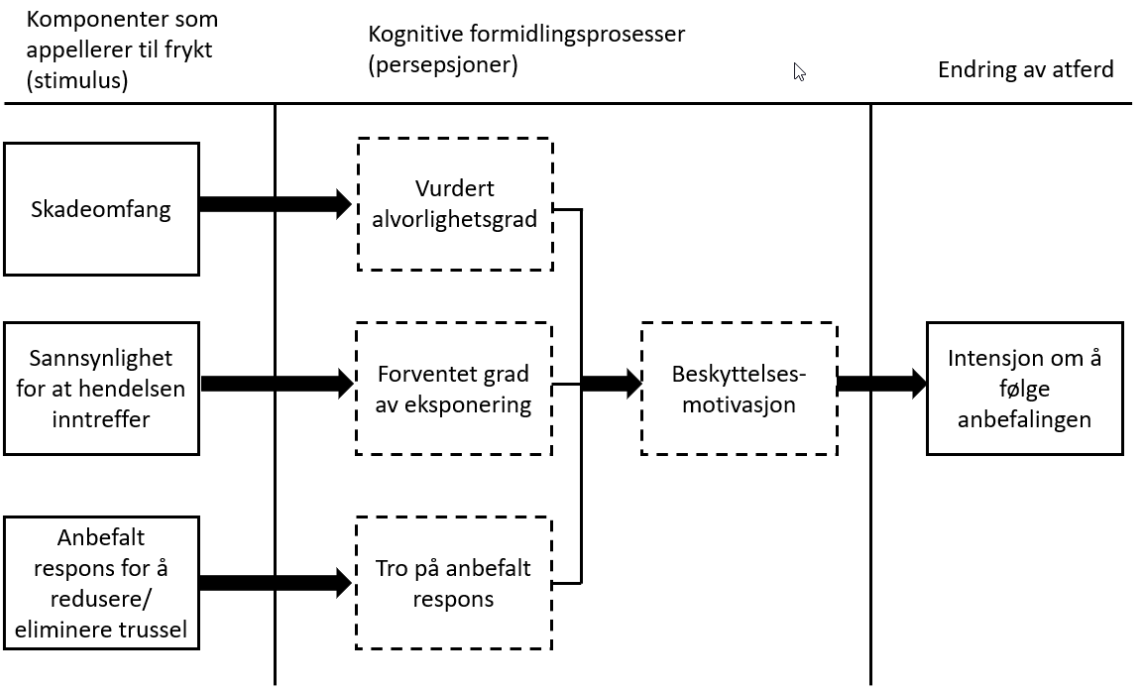
2.3.2 Theory of Rational Ignorance – Rasjonell uvitenhet

Begrepet *rasjonell uvitenhet* stammer fra Anthony Downs' bok fra 1957, «An Economic Theory of Political Action in a Democracy» (Downs, 1957). Bakgrunnen for begrepet var i utgangspunktet beregnet for å forklare velgeruvitenhet innenfor politikken. Downs hadde utfordringer med å forstå hvorfor så mange velgere var lite informert om viktige og relevante saker. Han konkluderte med at mange velgere følte at *kostnaden med å tilegne seg nødvendig kunnskap for å foreta et informert valg, ikke ga nok fordeler*. De fleste innså at selv om man brukte tid på å skape seg forståelse innenfor ulike temaer og valgte å stemme i samsvar med oppnådd forståelse – var det usannsynlig at det ville gi et annet resultat. Det er ingen av oss som har mulighet til å oppnå full forståelse innenfor alle temaer og vi prioriterer hva som er verdt å legge innsats i. Læringsmulighetene våre er uendelige, men det krever tid og energi.

Basert på sin litteraturstudie, konkluderte Barth og de Jong med at det var et bevisst valg for en person å ignorere konkret informasjon basert på en kost/nytte-vurdering, særlig i de tilfeller der innsatsen (kostnaden) uforholdsmessig oversteg de oppfattede og potensielle fordelene med å bruke tjenesten og/eller risikofaktorene knyttet til en eventuell feilaktig beslutning (Barth og de Jong, 2017). Barth og de Jong nevner et eksempel hvor brukere vurderte kostnaden for å lese gjennom lange og komplekse personvernregler til å være høyere enn hva de fikk av fordeler gjennom bruken av en aktuell tjeneste. Det tilsa at fordelen oppveide eventuelle bekymringer knyttet til mulig misbruk av personvernet.

2.3.3 Protective Motivation Theory (PMT) – Beskyttende motivasjon

Teorien om *beskyttende motivasjon* ble opprinnelig utviklet for å forklare effektene av hvordan frykt påvirket holdninger til helse og atferd. Teorien forklarer hvordan vi kan opprettholde vår beskyttende atferd og hvor selve motivasjonen til å beskytte seg blir et resultat av hvordan man opplever trusselen og et ønske om å unngå den (Rogers, 1975). I teorien finnes også en kost-/nytte-komponent der individet vurderer forholdsregler som må tas opp mot forventede fordeler før utøvelsen av aktuell atferd (Floyd, Prentice-Dunn og Rogers, 2000). Rogers selv forklarte teorien om beskyttende motivasjon gjennom underliggende modell (Rogers, 1975):



Figur 2.4: Teori for beskyttende motivasjon. Modellen er oversatt og modifisert for oppgavens behov (Rogers, 1975)

Ifølge Rogers var teorien om *beskyttende motivasjon* også koblet opp mot veletablerte teorier innenfor forventnings- og verditeorier. Tendensen for de alle var en funksjon av forventninger som følges av en konsekvens eller verdien av den (Rogers, 1975). Rogers henviste videre til Hovland et al.'s som foreslo tre viktige stimulusvariabler og forventings- og verditeorier som oppsto i situasjoner der det ble appellert til frykt:

1. Skadeomfang til en konkret hendelse
2. Sannsynligheten for at en hendelse inntraff hvis ikke anbefalt respons ble fulgt
3. Effekten av den beskyttende og anbefalte responsen hvor målet var å redusere eller eliminere trusselen

Basert på ovenstående stimuluskomponenter la man til rette for syv mulige kombinasjoner for å generere frykt i praksis. Og enhver effekt av kombinasjonene kan igjen være forårsaket av en eller flere komponenter. Videre ble det antatt at de tre stimuluskomponentene satte i gang hver sin kognitive formidlingsprosess:

1. Informasjon om skadeomfanget satte i gang en vurdering av alvorlighetsgraden
2. Sannsynligheten for at en hendelse inntraff, satte i gang en vurdering av hvor stor grad man var eksponert for hendelsen

3. Effektiviteten på den beskyttende og anbefalte responsen handlet om mestringstro på anbefalt respons.

Rogers hadde en hypotese om at prosessene var proporsjonale med styrken til den tilhørende stimulusvariabelen (Rogers, 1975). Imidlertid vil ikke resultatet være representativt for alle fordi vi vurderer trusler ulikt. I tillegg må en trussel bli oppfattet eller identifisert for at det skal være behov for å evaluere om man har evner og mestringstro i forhold til trusselen.

Analyser tilsa at beskyttelsesmotivasjon oppsto fra de kognitive prosessene på bakgrunn av (1) den konkrete hendelsen som kan føre til skade, (2) sannsynligheten for at den oppstår, samt (3) troen på å mestre den anbefalte responsen. Når motivasjon for beskyttelse var vekket, førte det til en intensjon om å utøve den anbefalte atferden med et mål om å redusere eller eliminere trusselen. Om en hendelse ikke ble vurdert til å være alvorlig, sannsynlig at den inntraff eller om ingenting kunne gjøres med den konkrete hendelsen, ble ikke motivasjon for beskyttelse vekket. Dermed oppsto heller ingen intensjon om å endre atferd. Rogers påsto at beskyttelsesmotivasjon var en multiplikasjonsfunksjon av de tre kognitive formidlingsprosessene av to grunner (Rogers, 1975):

1. Ingen motivasjon vil vekkes om noen av disse verdiene er lik null.
2. Forventingsteoriene til Atkinson, Edwards, Feather, Fishbein og Rosenberg hevdet også det multiplikative forholdet.

I hovedtrekk innebærer teorien om *beskyttende motivasjon* at folk vurderer alvorlighetsgraden og sannsynligheten for at man blir utsatt for en skadelig hendelse, samt at man vurderer ens evne til å håndtere aktuell hendelse og derfor endrer atferd basert på omstendighetene.

2.4 Teoretiske hypoteser

Det er en forventning om at de fleste ikke har noe forhold til de brukervilkår og personvern-erklæringer som man aksepterer underveis i en registrering eller en installasjon før bruk av smartklokken. Dette samsvarer med hva Williams, Nurse og Creese konkret nevnte i sitt studie (Williams, Nurse og Creese, 2019). Likevel er det interessant å undersøke nærmere hva man gjør for å beskytte egne helseopplysninger. Alle informantene jobber i en virksomhet som utvikler og selger tjenester knyttet til programvare som ute hos kunder vil inneholde sensitive personopplysninger. Dette betyr at alle har en profesjonalitet til det å vurdere skjerming av personopplysninger. Videre er det en forventning at flere synkroniserer data til

3. parter som for eksempel til andre treningsapp'er, men hvor bruken av 3. partens webside forventes å variere.

Derimot har jeg i denne eksplorative undersøkelsen ingen forventninger til hva som kommer opp av de beste og verste tenkelige scenarioene som smartklokkeprodusentene kan bruke ens helseopplysninger til, hverken i dag eller i morgen. Videre er det heller ingen forventning om at noen klarer å sette en konkret verdi på egne smartklokkedata.

2.5 Oppsummering

Dette kapittelet har definert og drøftet begrepet personvernparadokset, relaterte studier og teorier. Drøftingen over og problemstillingens natur aktualiserer tre ulike teoretiske perspektiver. Teorien om *planlagt atferd* baserer seg på individets holdning til atferden, subjektive normer og opplevd atferdskontroll. Disse tre elementene påvirker intensjonen og senere atferden. Mens teorien om *rasjonell uvitenhet* i korthet handler om at der innsatsen føles for høy, blir fordelene prioritert. Dermed velger man bevisst bort informasjon som kunne resultere i en annen beslutning enn den som er tatt. Den siste teorien som synes å være anvendbar i bacheloroppgaven er *beskyttende motivasjonsteori*. Her har man tre stimuluskomponenter som appellerer til frykt og hvor hver av disse fører med seg sin kognitive formidlingsprosess som påvirker motivasjonen til å beskytte seg slik at det blir relevant å endre atferd.

I kapittel 5 diskuterer vi de empiriske funnene i forhold til hypotesene/forventningene knyttet til de tre utvalgte teoretiske perspektivene og i forhold til følgende og mer presis formulering av problemstillingen:

> ***Hvilke vurderinger gjør smartklokkebrukere om bruksverdien til de sensitive persondata som ens smartklokke genererer?***

3. Metodiske opplegg

I dette kapittelet redegjør jeg for hvordan problemstillingen ble utviklet, hvilke valg som ble tatt i forhold til forskningsdesign, hvordan datainnsamlingen ble planlagt og gjennomført, samt hvordan analysearbeidet ble håndtert. Videre beskriver jeg hvordan jeg har ivaretatt dialogen med informantene med tanke på etikk, samt refleksjoner til studiens totale gyldighet.

3.1 Utviklingen av problemstilling

Interessen for personvern, helseopplysninger og bruk av smartklokker har vært med meg gjennom store deler av studiet. Bacheloroppgaven har derfor gitt en mulighet til å studere temaet mer i dybden og hvor jeg har fått mulighet til å gå fra teori til empiri. Som en følge av interesseområdet har jeg på forhånd samlet inn informasjon som kunne være relevant i utviklingen av problemstillingen. En problemstilling er det konkrete forskningsspørsmålet som studien skal finne ut av (Johannessen, Christoffersen og Tufte, 2011).

3.2 Valg av forskningsdesign

Metode er en teknikk og en fremgangsmåte som bidrar til å løse utfordringer og dermed skaper ny kunnskap. Johannessen, Christoffersen og Tufte skriver følgende om samfunnsvitenskapelig metode: «*Det dreier seg om å samle inn, analysere og tolke **data**, og dette er en sentral del av **empirisk forskning**. De viktigste kjennetegnene ved metode/ empirisk forskning er systematikk, grundighet og åpenhet*» (Johannessen, Christoffersen og Tufte, 2011). Samfunnsvitenskapelige metode skiller mellom kvantitativ og kvalitativ metode. Når man velger en kvantitativ metode handler det om å forske på noe som vil gi oss konkrete tall og hvor gjerne spørreundersøkelser blir benyttet som verktøy i forskningsprosessen. Kvalitativ metode derimot, handler om å samle inn ord og hvor det åpner opp for å gi en økt forståelse for et tema (Jacobsen, 2018).

Bacheloroppgaven baserer seg på en kvalitativ metode med en fenomenologisk tilnærming. Dette innebærer å forske på mennesker og deres erfaringer med et mål om å få en forståelse og innsikt i deres verden (Johannessen, Christoffersen og Tufte, 2011). I denne bachelor-oppgaven er det ønskelig å ha en dialog med informanter som har erfaring med og aktivt benytter en smartklokke. Bakgrunnen ligger i at smartklokker genererer helseopplysninger som puls- og søvnverdier og hvor disse er å anse som sensitive personopplysninger. Målet for dialogen er å forstå brukernes tanker om bruksverdien av data som genereres av deres smartklokker.

For å nå målet om forståelse, valgte jeg intervjuer som datainnsamlingsmetode. Jeg vurderte å gjennomføre fokusgruppeintervjuer fordi informantene har et fellesskap i bruk av smart-klokker. Imidlertid er ulempen med fokusgrupper at man får gruppesynspunkter og ikke de individuelle (Jacobsen, 2018). Av den grunn valgte jeg individuelle intervjuer. Verken observasjon eller dokumentundersøkelse var relevant i denne sammenheng.

For gjennomføring av intervjuene, valgte jeg semistrukturelle intervjuer som har en lav struktureringsgrad. Semistrukturelle intervjuer baseres på intervjuguider og gir mulighet for å bevege seg frem og tilbake i guiden under intervjuene (Johannessen, Christoffersen og Tufte, 2011). Ved å ha en lav struktureringsgrad, ga jeg indirekte informantene mulighet til å snakke så fritt som mulig, samtidig som jeg reduserte min rolle til det minste gjennom intervjuet for å begrense intervjueffekten. Samtidig ville intervjuguiden fungere som et hjelpemiddel og en rettesnor for å styre dialogen tilbake til spørsmålene om man havnet litt på utsiden av hva som opprinnelig var planlagt. Det sikret gjennomgang av alle spørsmålene og jeg føler det ga de beste forutsetninger for å besvare problemstillingen.

3.2.1 Valg av informanter

Med utgangspunktet i de begrensede ressursene jeg har hatt (er alene om bacheloroppgaven), har jeg begrenset meg til seks informanter og hvor utvalgskriteriene ble en kombinasjon av informasjons- og snøballmetoden. Informasjonsmetoden innebærer å plukke ut informanter man mener å ha mye å tilføre studien. Snøballmetoden er en slik informasjonsmetode og innebærer at man får tips fra en informant om andre relevante informanter man kan kontakte (Jacobsen, 2018).

Informantene mine er arbeidskollegaer som befinner seg innenfor min bekjentskapskrets. Det har vært en prioritering å rekruttere informanter blant relativt nyansatte og ansatte jeg ikke jobber nært med for å unngå mest mulig ulempene (svakere reliabilitet) med å bruke informanter fra egen organisasjon. I tillegg var det et mål å få til en god spredning på alder. Det viste seg dessverre at den yngre generasjonen ofte ikke benyttet klokke i det hele tatt eller ikke hadde smartklokke. Dermed innskrenket antallet av aktuelle informanter seg. Jeg hadde imidlertid et startpunkt hos en kollega som allerede i oppstarten av semesteret sa seg villig til å bidra fordi vedkommende synes dette var et interessant tema. I tillegg fikk jeg noe hjelp gjennom en intern snøballeffekt, der enkelte av informantene aktivt bidro til at flere sa ja til å være med på studien. Ett fellestrekk for alle disse, er at vi er ansatt i samme del av et selskap som utvikler elektronisk journalsystem innenfor helse- og sosialsektoren. Dette innebærer at

alle ansatte har grunnleggende kunnskap om skjerming av sensitive personopplysninger og tilhørende regelverk.

3.2.2 Intervjuguide

Intervjuguiden ble i hovedtrekk utarbeidet i parallell med utviklingen av problemstillingen. Jeg sørget for at spørsmålene bygget på hverandre og hvor jeg fulgte Johannessen, Christoffersen og Tuftes intervjufaser (Johannessen, Christoffersen og Tufte, 2011) med innledende spørsmål, overgangsspørsmål, nøkkelspørsmål, kompliserte og sensitive spørsmål, for deretter å trappe ned med et nytt nøkkelspørsmål og et avsluttende spørsmål.

Spørsmålene i intervjuguiden var som følger:

1. Hvilket smartklokkemerke har du?
2. Kan du beskrive hvilke bruksområder og nytte du har av smartklokken?
3. Det antas at du har laget din egen brukerkonto knyttet til smartklokken. I prosessen, brukte du noe tid på å lese brukervilkår/personvernerklæring? Hvis ikke - har du noen bakgrunn for at du valgte å ikke registrere deg?
4. For å logge på brukerkontoen din, logger du noen ganger på med Facebook- eller Google-kontoen din for å forenkle påloggingen? Hvorfor/hvorfor ikke?
5. Hvilke vurderinger gjør du i forhold til at data knyttet til aktivitet og søvn er å anse som helseopplysninger, altså sensitive data?
6. Pleier du å synkronisere dataene videre til en 3. part? Type Endomondo/Strava o.l? Hva tenker du om en eventuell risiko for spredning av dine helseopplysninger?
7. Hva tenker du om en eventuell mulighet til at analysevirksomheter, som f.eks. Google Analytics / Facebook Pixel, klarer å bygge en profil på deg basert på de data du avgir via smartklokken?
8. Hva mener du er de beste og verste tenkelige scenarioer som din smartklokke-produsent kan bruke dine helseopplysninger til i dag – og i morgen?
9. Hva tenker du om verdien på dine helseopplysninger? Og klarer du selv å sette noen verdi på egne data?
10. Vi har snakket mye om bruken og verdien av data. Hva tenker du etter denne dialogen? Vil du fremover ha mer fokus på brukervilkår og personvernerklæringer før du tar i bruk enheter som lagrer sensitive data?
11. Evaluering ved avslutning av samtalen: Tror du svarene dine hadde vært annerledes om du hadde fått spørsmålene i forkant av intervjuet?

I tillegg hadde jeg forberedt noen oppfølgingsspørsmål for å ha mulighet til å utforske nærmere om svarene ble kortfattede og for å ha mulighet til å opprettholde en god flyt i dialogen.

I forhold til siste spørsmålet er det alltid et dilemma ved intervjuer om jeg skal gi spørsmålene til informantene før intervjuet eller ikke. Gir man ut spørsmål i forkant, kan det føre til usikkerhet knyttet til svarene, om informantene tilpasser svarene til hva informanten tror du vil høre. På en annen side kan jeg få mer gjennomtenkte og reflekterte svar. Jeg valgte imidlertid å vente med spørsmålene til selve intervjuet for å få informantenes umiddelbare og ærlige respons. Samtidig ønsket jeg å høre deres evaluering slik at jeg tar med meg læringen til neste intervjusituasjon.

3.2.3 Intervju og transkribering

Når informantene valgte å si ja til forespørselen om å delta i studien, fikk de tilsendt informasjon om prosjektet, samt et samtykke som skulle signeres av den enkelte. Parallelt avtalte vi tidspunkt og sted for gjennomføring av intervjuet. Jeg hadde et ønske om å gjennomføre intervjuene fysisk og jeg valgte derfor å være fleksibel på både tid og sted for å gjøre det enkelt for informantene. Selve intervjuene ble gjennomført enten i kontorlokalene våre, hjemme hos meg eller på café.

Som en forberedelse til selve intervjuet ble informantene spurt om hva slags smartklokke-merke de hadde. På bakgrunn av informasjonen, lastet jeg ned smartklokkemerkets brukervilkår og personvernerklæringer. Dette slik at jeg ble kjent med de vilkår som gjaldt for den enkelte informant. Etter gjennomlesning av disse, laget jeg et notat på hvert klokkemerke hvor jeg beskrev egne tanker om vilkårene, samt noen relevante punkter fra vilkårene som kunne være greit å diskutere med informantene. For de to første informantene ble det tatt en gjennomgang av disse notatene. Det var planlagt å gjøre tilsvarende i de resterende intervjuene, men hvor jeg havnet i en situasjon der dette ikke var interessant for aktuell informant. For de resterende informantene valgte jeg å bake inn informasjonen underveis i intervjuene der dette var relevant. Siden de fleste informantene hadde Garmin, ble det enklere å få vilkårene inn som en del av intervjuet. Sannsynligvis førte dette til mer effektive intervjuer, da disse nå tok kortere tid.

I etterkant av hvert intervju gjennomførte jeg refleksjonsarbeid. Dette for å ivareta de første tankene etter intervjuet og hvor de muligens kunne bli viktige på et senere tidspunkt. Jeg noterte meg refleksjoner på selve intervjuet, samt en konklusjon basert på informantens

tilbakemeldinger. I tillegg vurderte jeg egen innsats under intervjuet. Etter ferdigstilt intervju, transkriberte jeg intervjuet som avtalt, samt at lydopptaket parallelt ble slettet.

Det ble gjennomført ordrett transkribering av hva informantene svarte, men kun i noen tilfeller av hva jeg selv sa. Transkriberingen skjedde i de tilfeller hvor vi var litt på sidelinjen av tema og hvor jeg ønsket at det skulle være mulig å se sammenhengen på et senere tidspunkt. Som en del av transkriberingsprosessen ble informanten fortløpende anonymisert og fikk tildelt informantnummer som erstatning. I etterkant av transkriberingen, noterte jeg også refleksjoner. Det å være fysisk i samtalen kontra det å transkribere samtalen i etterkant, ga nye tanker som var verdt å ta med seg videre. Oppdaget jeg ting under transkriberingen som kunne vært forbedret, var det fremdeles mulighet til å gjøre justeringer for de senere intervjuer. Når alle intervjuer og transkriberinger var ferdigstilt, ble det gjennomført en ny refleksjonsrunde som favnet rekrutteringsprosessen, intervjuguide- og innhold, intervjuene, samt egen innsats gjennom intervjufasen. Som en avslutning på intervju- og transkriberings-fasen, ble det sørget for at hver informant fikk en oppmerksomhet, enten i form av en påskeoppmerksomhet eller spandering av lunsj.

3.2.4 Analyse av de empiriske kvalitative data

Når intervju- og transkriberingsfasen var ferdigstilt, var det klart for neste fase hvor jeg skulle analysere tilbakemeldinger jeg hadde fått, samt vurdere hvilke beslutningsteorier fra litteraturstudien til Barth og de Jong (Barth og de Jong, 2017) det var aktuelt å koble både tilbakemeldinger og informanter opp mot.

Alle tilbakemeldinger som lå i transkriberingsfilene, ble flyttet over til Excel og hvor Excel ble benyttet som verktøy i analysefasen. Hvert spørsmål fra intervjuguiden fikk sin egen fane og hver tilbakemelding fra informantene ble lagt inn i respektive faner og med en kobling til informantnummeret. Av den grunn ble det enkelt å skifte fokus mellom spørsmål uten at man mistet koblingen til aktuell informant. Videre ble innholdet i hver tilbakemelding dekodet for lettere å sammenligne tilbakemeldingene. Hovedhensikten var å se om jeg fant grupperinger eller mønstre og dermed økt mulighet for å sammenligne tilbakemeldingene med hverandre. Der tilbakemeldingene var unike, ble de fanget opp i en «annet»-kategori for ivaretakelse i tilfelle disse senere skulle vise seg å være relevante. Når prosessen var gjort for alle spørsmål og tilbakemeldinger, var det mulig å skrive en oppsummering for hvert spørsmål på tvers av alle informantene. Oppsummeringen ble grunnlaget for videre bearbeiding på tvers av tema og ligger til grunn for funnene som presenteres i neste hovedkapittel.

Etter at jeg hadde analysert tilbakemeldingene fra informantene var oppgaven å vurdere både tilbakemeldingene og informantene opp imot hvilken beslutningsteori som er mest relevant for å tolke funnene. Her ble litteraturstudiet til Barth og de Jong (Barth og de Jong, 2017), i tillegg til Excel, benyttet som et verktøy.

3.3 Etiske vurderinger

Alle som skal håndtere personopplysninger i et forskningsprosjekt må søke Norsk senter for forskningsdata (NSD) om lov før man begynner datainnsamlingen. Som en del av bacheloroppgaven var det behov for å søke om å behandle navn og kontaktinformasjon til informantene, samt mulighet til å benytte lydopptak underveis i intervjuene for å konsentrere seg fullt i samtalene med informantene. Som en del av søknaden måtte jeg vedlegge intervjuguiden og et informasjonsskriv som skulle til informantene. Siden NSD har maler tilgjengelig for å sikre at søkere får med seg nødvendig informasjon ut til informantene, benyttet jeg én av disse som grunnlag. Informasjonsskrivet ble omdannet til mitt behov der jeg informerte informantene om hvordan jeg ville behandle deres personopplysninger og tilbakemeldinger i denne oppgaven, samt informerte de om hvilke muligheter som finnes om de senere ønsket å trekke seg fra prosjektet. I løpet av halvannen uke fikk jeg godkjennelse fra NSD og hvor alt nå var klart for å gå i gang med datainnsamlingen.

Når informantene takket ja til å bli med på studiet, sendte jeg informasjonsskrivet med samtykkeerklæring til de på epost som en forberedelse til intervjuet. Ingen av informantene stilte spørsmål om informasjonen og alle signerte samtykket i forkant av selve intervjuet. Jeg transkriberte alle intervjuene innenfor én uke etter gjennomført intervju. I den prosessen anonymiserte jeg både informant og virksomhet, samt at lydopptaket i etterkant ble slettet fra mobiltelefonen. Etter avtale med NSD, vil jeg slette transkriberingsfilene når jeg mottar endelig karakter for oppgaven. På bakgrunn av godkjennelsen fra NSD og hvor jeg følger opp skjermingen av mine informanter og deres tilbakemeldinger, anser jeg de etiske vurderinger i prosjektet som ivaretatt.

3.4 Studiens gyldighet og pålitelighet

For å gjennomføre en god studie, må vi reflektere over de valg som er gjort underveis og sørge for at valgene ikke påvirker vesentlig informasjonen som er samlet inn og/eller tolkning av den. For å si noe om den totale gyldigheten til en studie, vurderer man studiets pålitelighet til dataene og hvor god den begrepsmessige, interne og eksterne gyldigheten er (Jacobsen, 2018). Påliteligheten til dataene vurderes i forhold til hvordan data har blitt samlet inn,

analysert og til sist presentert. Er det spesielle forhold som har oppstått underveis og som kan påvirke resultatet, må dette opplyses om. Den begrepsmessige gyldigheten handler om at vi dokumenterer at vi måler det vi mener å måle. Den interne gyldigheten vises gjennom at vi klarer å etablere gode begrunnelser for de funn man presenterer, mens den eksterne gyldigheten vurderer muligheten til å overføre eller generalisere resultatene til andre sammenlignbare studier. I sum vil disse fire faktorene beskrive studiet totale gyldighet (Jacobsen, 2018).

3.4.1 Pålitelighet

Det har vært gode samtaler gjennom alle intervjuene og i noen grad ble jeg overrasket hvor stor åpenhet enkelte av informantene viste. Alle er erfarne og bevisste smartklokkebrukere og gjennom åpenheten vi hadde i samtalene, forventer jeg at tilbakemeldingene er sanne. Likevel har studien skjevheter som følge av at informantene er mine kollegaer og hvor jeg selv hadde rollen som intervjuer. I tillegg er det utvist åpenhet gjennom bruk av transkribering og tydelige beskrivelser av metodebruk. Basert på dette grunnlaget vil det være mulig å gjennomføre samme studie, med en annen forsker, et annet utvalg og hvor det lagt til rette for å sammenligne funnene.

3.4.2 Den begrepsmessige gyldigheten

Den begrepsmessige gyldigheten er forsøkt ivaretatt gjennom bruk av intervjuguide for å sikre at intervjuene ble gjennomført på tilnærmet lik måte. Jeg gjorde ingen revurderinger av spørsmålene i intervjuguiden fordi intervjuene fløt tilfredsstillende og det ble gode overganger mellom spørsmålene. Det ga meg senere en fordel fordi det ble enklere å sammenligne tilbakemeldingene i analysefasen. Selv om intervjuguiden fungerte etter intensjonen, hadde hvert intervju særegenheter og var unike. Likevel har studien en intervjueffekt i og med at jeg har en relasjon til alle informantene. Selv om det er søkt å redusere denne effekten ved å rekruttere kollegaer som er relativt nyansatte og noen man ikke jobber nært med til daglig, har man en relasjon som kan påvirke dialogen. Påvirkningskraften kan også falle innenfor kognitiv skjevhet der det er naturlig å ty til egen referanseramme både ved utvikling av spørsmålene og i selve intervjusituasjonen ved valg av ord og kroppsspråk. I tillegg har studien utvalgsskjevhet ved at aldersspennet ble smalere enn ønsket og hvor jeg antar at gjennomsnittsalder på de seks informantene ligger mellom 45-50 år. Selv om studien har skjevheter, er dette likevel forhold som er enkle å korrigere ved en eventuell ny og sammenlignbar studie.

3.4.3 Den interne og eksterne gyldigheten

Den interne gyldigheten er forsøkt sikret gjennom analysemetoden av dataene som er redegjort ovenfor.

Den eksterne gyldigheten går på om det er mulig å generalisere funnene fra studien og i kapittel 5 relaterer jeg funn fra denne undersøkelsen til andre empiriske undersøkelser. Det som er spesielt i min studie, er søkelyset på informantenes meninger og tanker om bruksverdien av egne helseopplysninger. Jeg forventer at funnene er gyldige om det gjennomføres tilsvarende studie på smarttelefoner. Som smartklokker, får smarttelefoner stadig mer avanserte helsefunksjoner og hvor sikkerheten for helseopplysninger er direkte sammenlignbare. Samtidig forventer jeg ikke at funnene er overførbare utenfor Norge. Selv om Europa har et felles regelverk innenfor behandling av personopplysninger (GDPR), må vi forvente at både kulturforskjeller og grad av tillit til samfunnsinstitusjoner vil kunne påvirke atferd og holdninger. Imidlertid er det bare ved å øke antall kvalitative og kvantitative studier på smartklokker som kan gi oss en bredere forståelse av dybden og bredden av «personvern-paradokset» som et sosialt fenomen.

3.4.4 Evaluering av den totale gyldigheten

I sum vil den totale gyldigheten av studien være preget av at informantene er mine kollegaer og en relasjon som kunne vært unngått ved en annen rekrutteringsprosess. Når det gjaldt valg av informanter, ble det et resultat av informasjon- og snøballmetoden og hvor alders-spredningen kunne vært bedre. Derimot var bruk av semistrukturert intervju et bevisst valgt for å få informantene til å snakke relativt fritt og for å redusere min påvirkningskraft underveis. Dette er faktorer som kan korrigeres om tilsvarende studie gjentas, for eksempel på smarttelefoner i stedet for smartklokker. Det vil gi muligheter for å teste om mine funn er overførbare.

På bakgrunn av åpenheten rundt de aktuelle skjevhetene, transkribering av intervjuene, tydelige beskrivelser på hvordan analysene er gjennomført og at det kan være mulig å teste overførbarheten opp mot smarttelefoner, anser jeg at den totale gyldigheten for min bacheloroppgave er så god den kan bli, sett i lys av de rammene en bacheloroppgave har.

3.5 Oppsummering

Gjennom metode-kapittelet har jeg beskrevet utviklingen av problemstillingen og begrunnet valget av en fenomenologisk tilnærming. Videre er valg av informanter beskrevet, spørsmålene fra intervjuguiden presentert, samt beskrevet hvordan jeg løste intervjuene og

transkriberingen. Til slutt presenterte jeg de etiske valgene som er tatt for å skjerme mine informanters opplysninger gjennom prosjektperioden og en vurdering av studiets totale gyldighet.

4. Presentasjon av funn

I dette kapittelet vil jeg presentere viktige resultater fra intervjuundersøkelsen og som ligger til grunn for å besvare oppgavens problemstilling.

4.1 Presentasjon av informantene

Jeg har intervjuet seks informanter, hvorav to kvinner og fire menn. Gjennomsnittsalderen ligger mellom 45-50 år og hvor intervjuene i gjennomsnitt varte i 43 minutter. Av de seks informantene var det hele fem som benytter Garmin smartklokke. Dog var det én av disse som benyttet Whitings i tillegg – men hvor den sistnevnte klokken ikke brukes til synkronisering med andre enheter. Den siste av informanten benytter Apple Watch i det daglige, men benytter Polar når vedkommende går på langrenn fordi Apple Watch ved denne aktiviteten har begrenset kartfunksjonalitet.

Presentasjon av informantene			
Informant	**Kjønn**	**Type smartklokke**	**Tid brukt på intervjuet**
Informant 1	M	Garmin	51 minutter
Informant 2	M	Apple Watch (Polar)	51 minutter
Informant 3	M	Garmin (Whitings)	35 minutter
Informant 4	K	Garmin	40 minutter
Informant 5	M	Garmin	42 minutter
Informant 6	K	Garmin	37 minutter

Tabell 4.1: Presentasjon av informantene

4.2 Bruksmønstre og nytte av smartklokken

For alle informantene er det relevant å logge egen aktivitet og hvor stor del av motivasjonen ligger i å måle diverse parametere og sammenligne økter, både for seg selv og med andre. For noen aktiveres konkurranseinstinktet og sporer til ekstra innsats. Bruken av GPS-data er også svært relevant, kanskje også litt eksklusivt i tilfeller der man har vært i utlandet og hvor man får god mulighet til å mimre om aktuelle økter i ettertid.

Kontrasten mellom de forskjellige aktivitetene til informantene er stor. Det er alt fra triatlon til sauesanking og soppturer. All aktivitet som krever innsats utover dagliglivet blir bevisst målt og track'et av alle informanter. For to av informantene blir også smartklokken aktivt benyttet i forbindelse med styring av næringsinntak hvor man har fokus på vektendring.

Imidlertid er det kun halvparten av informantene som bruker klokken gjennom hele døgnet. De som bruker klokken gjennom hele døgnet, muliggjør faste måleparametere som for eksempel antall skritt pr. dag, samt mulighet for å vurdere søvn. I tillegg er det én av informantene som aktivt benytter smartklokken i styring av både smarthus og el-bil. Den andre halvparten setter kun på seg smartklokken når de skal starte opp en aktivitet. For disse handler det om å få et annet fokus der man får mulighet til å koble av og kjenne på gleden ved sin aktivitet.

4.3 Tillit til håndtering av data

4.3.1 Smartklokkeprodusentene

Det var kun én av informantene som skummer brukervilkår og personvernerklæringer ved kjøp av ny smartklokke eller ved registrering av brukerkonto ved første gangs kjøp. Som en følge av dette, spurte jeg informantene om de implisitt har tillit til sin smartklokkeprodusent i forhold til at de håndterer deres data med respekt og i henhold til gjeldende regelverk. Alle bekreftet at de har tillit til produsenten. Både Garmin, Apple og Polar er store aktører i markedet og ingen ser derfor noen grunn til å mistro vilkårene de blir presentert for. Dessuten er det både krevende å lese alle sider med et juridisk språk, men det er også fordi alle ønsker å bruke funksjonene i den aktuelle klokken. Huker man ikke positivt av for vilkårene – får man ikke utnyttet de muligheter en smartklokke kan gi.

Derimot er halvparten av informantene svært bevisste på å lese og vurdere de andre innstillingene som senere følger av en installasjons- og/eller registreringsprosess. Gjennom denne prosessen gjøres det aktive valg. Dessuten var det også én av informantene som hadde registrert seg før det ble krav om å ha en gyldig epostadresse. Dermed har smartklokke-produsenten kun et brukernavn å forholde seg til, hvilket tilsier at det ikke er mulig å koble til en konkret person uten tillegg av andre data.

4.3.2 3. parters bruk av data

Det finnes gode datainnsamlingsmuligheter for en 3. part. Mange digitale løsninger innenfor privatmarkedet gir brukerne mulighet til å benytte forenklede påloginger, dvs. pålogging ved hjelp av for eksempel Facebook- eller Google-konto. Aktørene begrunner dette med brukervennlighet. Samtidig er det en kjensgjerning at dette bidrar til økt datainnsamling og hvor aktørene stadig lærer mer om sine brukere. Informantene i studien er bevisste i forhold til forenklet pålogging til smartklokkeprodusentens eller 3. partens websider. To av informantene var det ikke aktuelt for, enten fordi man kun benyttet app'en eller at man ikke

hadde mulighet fordi brukerkontoen ikke var koblet til en gyldig epostadresse. Mens de fire andre informantene var unisont enige – de ville aldri ha logget på hos aktørene ved hjelp av Facebook- eller Google-konto, samt at de sørger for å opprette egne brukerkontoer til ulike formål. Imidlertid var det to av disse informantene som innrømmet at de hadde benyttet forenklet pålogging i andre kontekster fordi man var i en situasjon der man skulle skynde seg.

Når det gjelder synkronisering til en 3. part var det fire av informantene som benytter Strava. Strava er kanskje den mest benyttede aktivtetsapp som finnes. De har hele 97 millioner brukere fordelt på 195 land og har 40 millioner opplastninger i uka (Strava, 2022). De to informantene som ikke benytter synkronisering til Strava, har automatisk fjernet risiko knyttet til at personlige opplysninger spres til ytterligere aktører. Samtidig er det ingen av de fire som ser noen risiko knyttet til den ekstra synkroniseringen. For de er nytten større enn den risikoen de føler. Én av de sier at det handler om tillit, mens en annen uttaler seg slik:

> *«Det er jo den største beskyttelsen vi har, tenker jeg: Jeg er ekstremt kjedelig! Det er liksom A4-metoden.»*

Basert på at brukerne synkroniserer data med flere aktører innebærer dette en ekstra mulighet for å lage en profil på deg som person, basert på dine data. Det var litt interessant at fire av informantene koblet dette umiddelbart til reklame og hvor to av disse heller vil ha tilpasset reklame så lenge man ikke spammes ned. Spørsmålet var imidlertid knyttet til det å lage en profil på deg som person basert på alle smartklokkedata – ikke bare kontaktinformasjon og eventuelt interesseområde. Én av informantene aksepterer at det er forretningsidéen deres, mens den siste informanten kommenterer at det ikke er lov med profilering. Og dette synes å være en korrekt tolkning av dagens GDPR-regelverk (Lovdata, 2018b). Profilering innebærer i hovedsak en automatisert behandling av dine personopplysninger og hvor informasjonen vil bli benyttet for å predikere dine fremtidige valg. Aktørene har anledning til å spørre om bruk av data. Imidlertid skal innsamlingen ha et konkret formål. Gis det samtykke fra brukere, har aktøren anledning til å samle inn ønsket og relevant informasjon og gis dermed anledning til å «massere» data for senere å levere tjenester til brukerne. Dog har ikke aktørene anledning til å samle inn data som går utover informert formål. Hvis så planlegges, må aktørene be om nytt samtykke fra brukerne.

I én av samtalene kom også miljøaspekter opp og hvorav det ene aspektet er relevant i denne sammenheng. All datainnsamling krever energiforbruk og ved synkronisering av data til 3. parter, bidrar man til økt datavolum – og dertil økt forbruk av energi. Dette kan muligens

bidra til at digitalisering i visse sammenhenger kan betraktes som en «ugrønn» aktivitet. Når Strava har 97 millioner brukere rundt om i verden tilsier dette at de sitter på ubeskrivelige mengder data som kan brukes i sammenhenger få har fantasi om.

4.4 Bruksverdien til smartklokkedata

Smartklokkene inneholder sensorer som fanger opp data vi som brukere av klokken benytter til å måle og sammenligne prestasjoner. Imidlertid er mange av dataene også definert som helseopplysninger, slik som for eksempel puls- og søvndata. Dette tilsier at man skal behandle disse dataene som sensitive. I denne konteksten er det ingen av informantene som bekymrer seg for at de bidrar til datainnsamling av helseopplysninger. Holdningen er generelt at man ikke har noe å skjule og at det gjøres vurderinger i forkant av smartklokkekjøpet. Har man først kjøpt en slik klokke, vil man bruke de funksjoner klokken kan gi. Spørsmålet som ofte kommer opp i intervjuene er:

> *«Hvilken glede kan andre ha av mine pulsverdier?»*

Spørsmålet bringer oss videre til hvilke gode scenarioer data fra smartklokken kan bidra til å løse i dagens og morgendagens samfunn. Her kommer forskning opp som én av de tingene som helseopplysningene kan bidra til. Om man gjennom et vitenskapelig datagrunnlag klarer å fremme forskning som gagner mennesker, er det en god ting å bidra med data. En annen god ting er at smartklokker kan inneholde sensorer som blant annet gir mulighet for å analysere hjertefrekvens, samt varsle om fall. Eventuelle fall kan varsles automatisk og vedkommende kommer direkte i dialog med noen som kan hjelpe. Dette kan bidra til økt trygghet for de som har bekymringer knyttet til fall. Trygghet vil det også gi om klokken er i stand til å advare deg om det skjer endringer i verdier som tilsier at sykdom er på gang i kroppen, men som man foreløpig ikke merker selv.

Temaet «forsikringsselskaper» kom opp både som et godt og et dårlig scenario. For det gode kan det være at en selv får fordeler av å dele helseopplysninger med forsikringsselskapet. Imidlertid vil dette kreve samtykke fra smartklokkebrukeren og fordeler kan vise seg gjennom for eksempel rabattordninger. Om man ser dette fra den andre siden, vil det komme dager hvor helsen ikke lenger er den samme. Løsningen kan være å ikke ha en smartklokke eller å ikke dele helseopplysninger med forsikringsselskapene. Det kommenteres fra én informant at selv om de store forsikringsselskapene oppleves som ryddige, dukker det innimellom opp nye forsikringsselskaper som vil trenge tid for å bygge opp tilsvarende tillit.

Det kom kun én tilbakemelding på et scenario hvor noen kan misbruke ens helseopplysninger – og det var forsikringsselskaper. Resten av informantene hadde ingen svar på hva som var det verste scenarioet i dag – og i morgen. Hele fire av seks informanter, kommer med svar som knyttes til GPS-data heller enn helseopplysninger. Dette selv om GPS-data ikke er særs beskyttet i lovverket. Dette er en personopplysning og håndteres som det i lovverket, men ansees ikke som sensitive opplysninger alene. Tre av disse fire informantene nevner at hvis noen har tilgang til ens GPS-data, vil en vite når man er borte fra egen husstand. Da er det mulig at uvedkommende som har fått tilgang til denne type data kan bryte seg inn i boligen. Én av disse fire informantene drar det litt lengre og sier at det verste vil være å bli track'et gjennom hele døgnet og hvor man ikke har anledning til å skru av sensorer og dertil eventuell lagring av data. Gjennom informasjon kan man etter hvert skape et mønster som en «con artist» kan gjøre seg bruk av. Det innebærer at noen vet så mye om deg og ditt mønster, slik at man naturlig kan opptre som deg og svarer naturlig på de spørsmål som identifiserer deg. Den siste av de fire informantene knytter GPS-data til det militære og hvor man kan ha høytstående befal eller spesialsoldater i Norge som benytter Strava. Som en følge av dette kan man risikere å avsløre hemmelige installasjoner eller tilsvarende. På bakgrunn av dette, vil data fra Strava være interessante etterretningsdata. Så har også skjedd. Allerede i 2018 ble det avslørt at man kunne benytte Strava-data til å røpe lokalisering av baser og hvem soldatene er (Lied og Svendsen, 2018). Men igjen, dette handler om GPS-data, men altså ingen klarer å dra de verste scenarioene for misbruk av helseopplysninger lenger enn til uheldig bruk fra forsikringsselskapene.

4.5 Helseopplysningenes verdi

Det er altså ingen av informantene som ser noen verdi av sine helseopplysninger eller klarer å sette noen verdi på egne data. Dog var det én av informantene som tenker at det hadde vært annerledes om man hadde hatt på seg smartklokken døgnet rundt. Her er man igjen på GPS-data og hvor vedkommende er svært bevisst på å skru av sporingen når det ikke finnes konkrete behov som skal løses.

Bakgrunnen for at informantene ikke ser verdien av helseopplysningene, er at man ikke helt klarer å se hva de kan bli brukt til, annet enn at man får historikk over tid. I tillegg konkluderte én av informantene:

> «*Men at man kunne få betalt for det liksom, for å gi fra seg helseopplysninger, den sitter vel lengre inne for en amatør*.»

Det er verdien av selve produktet som er viktig for informantene – ikke det at de selv bidrar til en form for datainnsamling. Noen av informantene er aktivt med i community eller samfunn på Strava. Én av disse har en relativt åpen profil, hvilket innebærer at andre kan se vedkommende aktivitet. Imidlertid kan vedkommende også se andres profiler – og har stor glede av det. Dette gjelder spesielt i form av å finne frem til nye sykkelstier. Dette gir både inspirasjon og motivasjon og vedkommende tenker:

> «*For å få, må jeg gi noe tilbake.*»

Spørsmålet om helseopplysningenes verdi, trigger likevel noen tanker. Én av informantene mener det ville fått konsekvenser for smartklokkeprodusentene om brukerne unisont hadde nektet datainnsamling og hvor brukerne av den grunn la hindringer for både videreutvikling og inntjening, men dette ville ha gitt et mindre funksjonelt produkt. Og om det skulle dukket opp situasjoner der det ryktes om lekkasjer fra en smartklokkeprodusent, ville det vært svært uheldig. Samtidig deler mange informasjon aktivt og hvor det publiseres på Facebook, Instagram m.m. når man er fornøyd med en treningsøkt. En annen informant skulle gjerne hatt tilgang til volumet av treningsdata for selv å jobbe med maskinlæring og statistikkhåndtering av disse.

4.6 Evaluering på slutten av intervjuet

På tampen av intervjuene spurte jeg informantene om de ville ha mer fokus på brukervilkår og personvernerklæringer når man frem i tid tok i bruk nye enheter som lagrer sensitive data. Fire av seks informanter sier at de fremover ikke vil ha mer fokus på disse. Det er for mange sider med juridisk språk og som er dekkende for å holde i en eventuell rettsak, samt at man ikke har noen mulighet til å påvirke. Derimot hadde én av disse informantene tenkt over Schrems II-dommen (Digitaliseringsdirektoratet, u.å.) og hvor vedkommende foreløpig ikke hadde sjekket ut Garmin – men som nå ville bli gjort. Samtidig sier én annen av informantene at man har tatt et valg før kjøpet ved å stole på aktuell smartklokkeprodusent og at man derfor ikke velger å bruke tid på disse vilkårene.

Imidlertid var det én av informantene som svarte ja på dette spørsmålet. Dette var samme informant som vedkjente å ha skummet vilkårene. Vedkommende har erfaring fra GDPR og databehandleravtaler og føler ofte at man har mer fokus på temaet enn mange andre. Den siste informanten ga et overraskende «*kanskje*». Samtalen hadde bidratt til å gi mer bevissthet slik at man muligens sjekket ved kjøp av en ny smartklokke. Men, fremdeles var det en erkjennelse at man ikke klarer å se hvordan disse dataene kan skade en. Vedkommende ser

mer på at dataene kan være til hjelp i form av jevnlige oppsummeringer. På den måten kan man faktabasert følge med på status og sammenligne økter – både for seg selv og med andre. Oppfatningen, som deles med flere, er at det å være en del av et community er verdifullt når det gjelder å holde motivasjonen oppe og hvor det i sum resulterer i bedre helse.

Som læring for egen del, spurte jeg også om tilbakemeldingene ville blitt annerledes om de hadde fått spørsmålene i forkant. Alle var enige i at tilbakemeldingene i hovedsak ville ha vært det samme, dog ville noen tilbakemeldinger ha blitt lengre, andre kortere og mer presise, mens flere ville tatt seg tid til å sjekke brukervilkårene og personvernerklæringene i forkant av intervjuene. Én av informantene kom også med en konkret tilbakemelding knyttet til at intervjuet var passe langt og at det var fint å få opp bevisstheten rundt temaet. Det var lettere å reflektere over spørsmålene som går på en selv, i stedet for å lese en artikkel.

4.7 Sammenfatning av intervjuene

Funnene i studien er basert på et utvalg på seks informanter som gir oss deres tanker og vurderinger om bruksverdien til sine smartklokkedata. Funnene tilsier at smartklokke-produsentene og 3. parten, Strava, innehar stor tillit blant brukerne og hvor informantene har liten fantasi på hvordan deres helseopplysninger kan misbrukes. Dermed klarer de heller ikke å sette noen verdi på egne helseopplysninger. På tampen av intervjuene var det likevel en liten bevegelse når det gjelder å gjøre seg kjent med brukervilkår og personvernerklæringer ved neste kjøp. Under vises en oppsummering av de viktigste avklaringene etter analysefasen (In = Informantnummer n):

Personvernparadokset og bruk av smartklokker						
Beskrivelse	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**
Bruk - logging/sporing av trening	Ja	Ja	Ja	Ja	Ja	Ja
Bruk - næringsinntak	Nei	Ja	Nei	Nei	Nei	Periodevis
Klokken brukes hele døgnet (=søvn)?	Ja	Ja	Nei	Nei	Nei	Ja
Leser bruksvilkår og personvernerklæring?	Nei	Nei	Nei	Nei	Nei	Skummer
Vurderer andre innstillinger?	Ja	Ja	Ikke avklart	Ja	Ikke avklart	Ja, men ikke konsekvent
Tabellen fortsetter på neste side.						

Tabell 4.2: Oversikt over analyserte svar fra informantene - del 1 av 2

Tabellen fortsetter fra forrige side.

Personvernparadokset og bruk av smartklokker						
Beskrivelse	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**
Koblet til eksisterende konto?	Ja	Ja	Ja	Ja	Ja	Ja
Tillit til smartklokkeprodusent?	Ja	Ja	Ja	Ja	Ja	Ja
Logger du på med FB/Google-konto?	Aldri	Ikke relevant	Aldri	Ikke relevant	Aldri	Aldri
Oppretter egen brukerkonto?	Ja	Ikke relevant	Ja	Ikke relevant	Ja, i trenings-øyemed	Ja, i trenings-øyemed
Bekymret for dine helseopplysninger?	Nei	Nei	Nei	Nei	Nei	Nei
Synkroniserer med 3. parter?	Ingen	Strava	Strava	Ingen	Strava	Strava
Tanker om risiko for spredning av helseopplysninger?	Ikke relevant	Ingen	Ser ingen risiko	Ikke relevant	Handler om tillit	Ser ingen risiko
Har dine helseopplysninger noen konkret verdi?	Nei	Nei	Nei	Nei, men…	Nei	Nei
Etter dialogen – har du mer fokus på brukervilkår og personvernerklæring?	Nei	Nei	Kanskje	Nei	Nei	Ja, er med på å øke bevisstheten

Tabell 4.3: Oversikt over analyserte svar fra informantene - del 2 av 2

4.8 Oppsummering

I dette kapittelet har jeg presentert funnene fra samtalene med mine informanter. Hoved-funnene er at informantene bryr seg lite om brukervilkår og personvernerklæringer. Derimot er de bevisste på å vurdere resterende brukerinnstillinger som fremkommer i en installasjon- og/eller registreringsprosess, samt å lage egne brukerkontoer til forskjellige formål. Samtidig har informantene tillit til at smartklokkeprodusentene håndterer deres data i henhold til regelverket og har ingen bekymringer knyttet til at deler av smartklokkedataene er helseopplysninger. Imidlertid tenker de mer på GPS-data enn helseopplysninger og skulle andre kjenne deres GPS-data, føles det mer invaderende. Likevel ser ikke informantene hvordan deres helseopplysninger kan misbrukes, hverken på kort eller lang sikt. Av den grunn, ser de heller ikke bruksverdien av egne helseopplysninger.

5. Drøfting av funn

Det er mange studier som har personvernparadokset som tema, men det er få som tangerer min problemstilling og som dermed kan brukes for å sammenligne mine funn med empiriske resultater fra tidligere studier

Forskerparet Barth og de Jong studerte personvernparadokset i forhold til et antall mulige generiske beslutningsteorier. De konkluderte med at det var behov for å benytte både rasjonelle og irrasjonelle beslutningsteorier for en beslutningsteoretisk forståelse av personvernparadokset. I tillegg mente de at god design på digitale grensesnitt bidro til at brukerne selv sørget for økt beskyttelse av egne data (Barth og de Jong, 2017).

Williams, Nurse og Creese utviklet et smartklokkespill for å øke kunnskapen om personvern. Deres mål var å forklare smartklokkebrukernes atferd gjennom bruk av teorien om beskyttende motivasjon. De konkluderte med at det var trusselskomponentene som hadde den største påvirkningskraften (Williams, Nurse og Creese, 2019). Selv om brukerne hadde et balansert forhold til alvorlighetsgraden, viste forskerne til at de informerte brukerne, de som hadde spilt smartklokkespill med personverntillegget, kategoriserte data og vurderte det til at deler av dataene kunne deles, mens andre burde beskyttes. På bakgrunn av dette konkluderte de med at smartklokkespill med personverntilpasninger bidro til å øke bevisstheten i forhold til personvern (Williams, Nurse og Creese, 2019). Williams, Nurse og Creese påpekte imidlertid at det ikke har vært noen empiriske studier knyttet til personvern for smartklokker (Williams, Nurse og Creese, 2019). Likevel refererte de til studien til Udoh og Alkharashi (Udoh og Alkharashi, 2016) som var den mest relevante studien i forhold til problemstillingen min.

Udoh og Alkharashi fokuserte på holdning og bevissthet til personvern, samt hvordan disse faktorene påvirket atferd i forhold til bruk av smartklokker (Udoh og Alkharashi, 2016). De påviste at bekymringer rundt personvernet korrelerte med ens holdning til personvern generelt og hvor det også viste seg at kulturell bakgrunn påvirket holdningen til personvern. Dette er den eneste studien som nærmet seg spesifikt helsedatadelen av smartklokkene og hvor informantene argumenterer for at det er forskjellige nivåer av sensitivitet knyttet til dataene som genereres. Flere av informantene uttrykte en «*jeg har intet å skjule*»-holdning (Udoh og Alkharashi, 2016) akkurat som jeg finner her.

5.1 Personverninnstillinger

Etter at man har gått til innkjøp av en smartklokke, vil det være behov for å konfigurere klokken etter individets ønskede bruk. Det være seg data som høyde, vekt, type aktiviteter og eget ambisjonsnivå i forhold aktivitet og søvn. Som en følge av oppstartsprosessen er det vanlig å måtte akseptere brukervilkår og smartklokkeprodusentens tilhørende personvern-erklæringer. Svarer man nei på disse, kan man ikke forvente å ha en smartklokke som tilbyr full funksjonalitet og kjøpet kan i verste fall være bortkastet. Dessuten, man går ikke til innkjøp av en smartklokke kun for å få vist tid og dato. Av funnene i oppgaven var det som forventet få som gjorde seg kjent med informasjonen underveis i oppstartsprosessen. Det var kun én informant som skummet informasjonen og vedkommende hadde allerede god kjennskap til GDPR-regelverket. Dette bekreftes også fra studiet til Barth og de Jong og med teorien *rasjonell uvitenhet* (Rational Ignorance Theory). Dette innebærer at et individ bevisst kan velge å ignorere informasjon basert på en kost-/nytteberegning. Forskerne nevnte konkret at kostnaden ved å lese kompliserte vilkår i sin helhet kan kreve for mye tid og innsats og man bestemmer seg for at fordelene oppveier eventuelle bekymringer knyttet til personvernet (Barth og de Jong, 2017). Den ene informanten som valgte å skumme vilkårene er støttet gjennom teorien om *planlagt atferd* (Ajzen, 1991). Vedkommende har, som nevnt, god kjennskap til GDPR og har derfor både en holdning til at man bør gjøre seg kjent med gjeldende vilkår og hvor dette også forventes av en selv. I tillegg har vedkommende trygghet for at man takler de eventuelle utfordringer som måtte oppstå. Begge faktorene gir en intensjon om å utøve en gitt atferd – altså å lese de vilkår en blir presentert for.

Selv om man bevisst velger å overse brukervilkårene og personvernerklæringene, er det mer fokus fra informantene knyttet til resterende innstillinger. Her gjøres aktive vurderinger og man er svært bevisste på hvilke valg som gjøres og hva man selv ønsker. Ved visse tilfeller er det ønskelig å bli eksponert for informasjon og man velger å takke ja ved slike valg-muligheter. Mens i andre sammenhenger velger man bort informasjon og bidrar ikke til smartklokkeprodusenten og 3. partens datainnsamling. I tillegg var informantene svært bevisste i forhold til selve bruken av aktørenes app og websider. Blant annet opprettet de alltid egne brukerkontoer for treningsaktivitet for å unngå sammenblandinger. I tillegg benyttet de aldri, i treningssammenheng, forenklet pålogging der man gis mulighet til å logge på med f.eks. Facebook- eller Google-kontoen i stedet. Dette vitner om god forståelse om sikkerhet rundt bruken av sosiale medier. I og med at det gjennomføres aktive vurderinger fra informantene, indikerer dette at de er rasjonelle i sin vurdering av risiko.

Denne type atferd samsvarer med hva Barth og de Jong hevdet i teorien om *planlagt atferd*, hvor sterke holdninger, opplevd kontroll og etterlevelse av sosiale normer førte til at et individ engasjerte seg i en viss atferd (Barth og de Jong, 2017). Både informantenes holdning til atferden de utviser i denne sammenheng og at de selv aktivt tar rollen med å gjøre nødvendige endringer på mulige brukerinnstillinger, vil påvirke deres intensjon og dermed også deres handlingsmønster. Derimot ser jeg ingen kobling til subjektiv norm. Av hva jeg tolker ut fra samtalen med informantene, står de godt i egne beslutninger om type handling og jeg observerer ingen tegn til at de lar seg påvirke av en sosial norm. Selv om informantene ikke oppleves som at de er preget av noen sosial norm, vil deres atferd likevel støttes gjennom teorien om planlagt atferd, da både holdningen til atferd, subjektiv norm og persipert atferds-kontroll ansees som uavhengige komponenter til å påvirke intensjon og atferd (Ajzen, 1991).

5.2 Tillit til håndtering av mine data

Det var en unison enighet om at man har tillit til smartklokkeprodusenten når det gjelder deres håndtering av egne data. Situasjonen hadde kanskje vært annerledes om det hadde vært flere aktører med i bildet. Alle aktørene, Garmin, Apple Watch og Polar, er store aktører og har en stor andel av markedet innenfor smartklokker. Det samme gjelder Strava som er den eneste parten som benyttes i de tilfeller man synkroniserer til en 3. part.

Samtidig, med at disse aktørene er blant de største i markedet, vil det innebære at de parallelt sitter på en enorm mengde data. Bruk av kunstig intelligens og Big Data kan fungere som gode verktøy og vil gi aktørene tydelige trender og samtidig mulighet til å oppdage mønstre som kan gi nye forretningsmuligheter. Jeg antar at det i hovedtrekk er populasjoner som er interessante og ikke enkeltindivider. Men vet vi egentlig det? For med verktøyene som finnes og aktivt benyttes i markedet, samt få og store eiere, gjør det mulig å både fremskaffe og sammenstille data fra forskjellige kontekster. Selv om mesteparten av data som samles inn i utgangspunktet ikke er sensitive, kan en sammenstilling av data likevel utvikle seg til å bli sensitive (Datatilsynet, 2013). Det som ble et overraskende funn, var at ingen av informantene bekymrer seg for at de bidrar inn i en storstilt datainnsamling av helseopplysninger, som er sensitive i utgangspunktet. Holdningen er at de har intet å skjule og ingen klarer å se verre scenarioer enn at forsikringsselskaper får tilgang til disse dataene. Samtidig bidrar også forsikringsselskaper til mulige gode scenarioer. Dette i tilfelle om datainnsamlingen fanger opp mønstre som gjelder ens egne helseopplysninger som man foreløpig ikke merker selv, samt mulige rabattordninger. Vi har to ytterpunkter av perspektiver på forsikringsselskaper.

Likevel har informantene en enighet om at man ikke er bekymret for helseopplysningene sine. De stiller seg egentlig spørsmålet om hvilken glede andre kan ha over ens egne pulsverdier.

Det kan være relevant å koble denne tankegangen til studiet til Udoh og Alkharashi, selv om disse ikke støtter seg på noen spesifikk teori. De erfarte også «*intet å skjule*»-holdningen og de fant ut at bekymringer knyttet til personvern korrelerte med ens egen holdning til personvern generelt (Udoh og Alkharashi, 2016). Samtidig er det store ulikheter mellom disse studiene. Deres studie er foretatt i aldersgruppen 19-26 år og hvor de har tilknytning til et studiested, mens jeg har intervjuet kollegaer som har en antatt gjennomsnittsalder mellom 45-50 år. Dette innebærer at jeg har en forventet ulikhet med tanke på bruk av sosiale medier, men også ulikhet i forhold til livserfaring. Når jeg i tillegg tar hensyn til kunnskapen om at informantene jobber i en virksomhet som har høy bevissthet rundt skjerming av persondata, har jeg ikke tilsvarende korrelasjon mellom bekymringer og holdning til personvern som Udoh og Alkharashi erfarte. For å finne støtte i teori, er det aktuelt å hente paralleller fra studien til Williams, Nurse og Creese. De benyttet teorien om *beskyttende motivasjon* og fant at det var trusselskomponentene i teorien som hadde den største innflytelsen (Williams, Nurse og Creese, 2019). I og med at mine informanter ikke er bekymret over dataene som samles inn av aktørene, innebærer det at om eventuelle hendelser inntreffer – har ikke dette noen høy alvorlighetsgrad. Dermed er trusselskomponenten som Williams, Nurse og Creese nevnte, tilnærmet fraværende. Og når Rogers hevdet at beskyttelsesmotivasjonen er et resultat fra en multiplikasjonsfunksjon mellom de tre kognitive formidlingsprosessene (Rogers, 1975), vil jeg konkludere med at beskyttelsesmotivasjonen ikke vil vekkes for mine informanter, all den tid vurdert alvorlighetsgrad er tilnærmet null. Dermed oppnår man heller ingen endring av atferd.

5.3 Dataens bruksverdi

Som tidligere nevnt samler de store aktørene inn gigantiske mengder data og som smartklokkebrukerne er en bidragsyter til, sammen med andre enheter og app'er. Datatilsynet påpeker ubalansen og sier allerede i 2013 (Datatilsynet, 2013):

> «*Det er de virksomhetene som **samler inn** personopplysninger som henter ut den stadig voksende merverdien som ligger i analyse og bearbeiding av disse opplysningene, og ikke vi som **avgir** opplysningene. Snarere kan denne transaksjonen være til forbrukerens ulempe i den forstand at den kan utsette oss for potensiell fremtidig sårbarhet.*»

I samme rapport skriver også Datatilsynet at OECD jobber for å finne en metode som kan være med å bidra til å avklare verdien på personopplysninger. Dette vil bidra til åpenhet og innsikt på hvordan et marked for personopplysninger fungerer og dermed også en mulighet for forbrukerne til å lære og forstå mekanismene. På den måten vil forbrukerne bedre se at ens egne data har en verdi i seg selv. Økt kunnskap vil videre bidra til å redusere ubalansen mellom de store aktørene og forbrukerne. Med kunnskap følger mulighet til å stille reelle krav og hvor man som forbruker gis en mulighet til å påvirke de store aktørene i markedet.

Selv om dette er en rapport som ligger hele 9 år tilbake i tiden, er det fremdeles ingen allmenn forståelse at våre data har noen verdi i seg selv. Samme forståelse har alle informantene i forhold til egne helseopplysninger. Derimot var det én av informantene som mente at det hadde vært annerledes om man benyttet smartklokken hele døgnet og hvor det gir en helt annen mulighet til sporing. Imidlertid var det her henvisning til sporing gjennom GPS-data, ikke vedrørende ens helseopplysninger. Vi kan igjen trekke paralleller til Williams, Nurse og Creese som benyttet teorien om *beskyttende motivasjon* (Williams, Nurse og Creese, 2019) og hvor det var trusselskomponentene som var den mest påvirkelige variabelen. Når ingen av mine informanter klarer å se noen verdi i egne helseopplysninger fra smartklokken, vil trusselskomponenten være helt fraværende. Og på grunn av Rogers påståtte multiplikasjons-forhold (Rogers, 1975), vekkes heller ikke beskyttelsesmotivasjonen og man har ingen motivasjon til å endre atferd.

Blant de gode scenarioene for bruk av våre helseopplysninger fremover i tid, ble det nevnt at man kan oppnå rabattordninger om man utveksler helseopplysninger med forsikrings-selskapene. Potensielle rabattordninger vil gi dataene en bruksverdi og muliggjør målinger i «kroner og øre». Foreløpig er ikke «smarte» helseforsikringer tilgjengelig i Norge. Imidlertid har allerede Garmin en avtale med det globale forsikringsselskapet SCOR Global Life hvor det benyttes Garmin-klokker for å samle inn aktivitet- og helsedata (Anderssen, 2019). Forsikringspremien vil bli lavere om du lever sunt, samt at du får tilgang til en helsecoach. Teknologien er her, så tilbudet til forbrukermarkedet avhenger nok av hvor modne vi er og hvor stor tillit vi har til våre forsikringsselskaper. Fremover vil vi, på en eller annen måte, bli tvunget til å ta stilling til bruksverdien av våre personopplysninger.

5.4 Potensiell endring i atferd

Når intervjuene nærmet seg slutten, var det litt spennende om jeg underveis hadde trigget noen tanker som kunne gi seg utslag i informantenes fremtidige atferd vedrørende vern av

egne helseopplysninger. To tredjedeler var tydelig at de ikke kom til å ha ytterligere fokus enn hva de allerede hadde, mens den resterende delen var litt på glid. Tilsvarende resultater ble erfart i flere studier. I studien til Williams, Nurse og Creese viste det seg at behandlingsgruppen lærte å gjøre tiltak for å beskytte egne data gjennom smartklokkespillet, mens kontrollgruppen var tilnærmet på samme ståsted som tidligere (Williams, Nurse og Creese, 2019). I studien til Udoh og Alkharashi innrømmet deres informanter på slutten av intervjuet at de også hadde behov for et privatliv. Imidlertid hadde de ikke bedre forklaringer enn at de ikke forventet noen brudd på personvernet. Derimot var deres informanter mer opptatt av å skjerme mobiltelefonen (Udoh og Alkharashi, 2016). Løsningen kommer kanskje fra Williams, Nurse og Creese sin studie hvor det nevnes at det fra tidligere arbeider ble foreslått at manglende oppmerksomhet knyttet til personvern, kan løses gjennom å øke oppmerksomheten (Williams, Nurse og Creese, 2019). Det tilsier at både studiet til Udoh og Alkharashi, samt min bacheloroppgave har bidratt i den sammenheng med å påkalle informantenes oppmerksomhet gjennom intervjuer. Bidrag for å øke bevisstheten, gjør også Datatilsynet gjennom sin Personvernblogg. I blogginnlegget fra april, ble det henvist til et utsagn fra Umberto Eco på 1980-tallet: «*Den største utfordringen er ikke å sikre personvernet til de få som ber om hjelp, men å få alle andre til å betrakte personvernet som et verdifullt gode*» (Dahl, 2022).

5.5 Personvernparadokset

Som jeg nevnte i kapittel 5.1, går man ikke til innkjøp av en smartklokke kun for å få en klokke som viser tid og dato. Man ønsker mer funksjonalitet og samtykker til de vilkår som finnes for å benytte eksisterende funksjonalitet – og ønsker gjerne stadige forbedringer. Det er en kjensgjerning at hovedmålet er bruk av smartklokken – ikke vurdering av personvern. Som en følge av dette får personvernet automatisk en lavere prioritet og som støttes av Hughes-Roberts som skrev at personvernet hadde utfordringer fordi det var et sekundært mål (Hughes-Roberts, 2015). Gjennom studien beviste han at et bedre digitalt grensesnitt, ga brukerne en effekt ved at sensitiv informasjon lettere ble identifisert og hvor det ga brukerne økt kontroll over egne data. Barth og de Jong konkluderte også at god design i et grensesnitt var et krav om man skal klare å være rasjonell i forhold til eget personvern (Barth og de Jong, 2017). Solove uttrykte seg innenfor samme tema, da han ikke hadde tro på at individer bør få ytterligere muligheter til å justere valgene sine, men at man heller må konsentrere seg om arkitektur og struktur når det handler om bruk, vedlikehold og overføring av data (Solove, 2021).

Parallelt med utfordringer knyttet til personvernet, beveger verden seg stadig raskere i forhold til digitalisering. De to siste årene har det vært en voldsom vekst knyttet til digitale krav som har oppstått som følge av Covid19-pandemien og behovet for å få samfunnet til å fungere tilnærmet best mulig i en særs spesiell situasjon. Hva som ble ment som en definisjon på personvernparadokset i 2001, kan ha et annet grunnlag i dag. Samtidig finnes det ingen ens definisjon av begrepet eller fenomenet. Derimot hadde Buttarelli en definisjon av hva personvernparadokset er – og ikke er. På en internasjonal konferanse i 2018, hvor tema var «*Verdighet og respekt i en datadreven verden*», hadde Buttarelli åpningstalen (Buttarelli, 2018). Her fremførte han sin forståelse:

> *The so-called 'privacy paradox' is not that*
> *people have conflicting desires to hide and to expose.*
> *The paradox is that we have not yet learned how to*
> *navigate the new possibilities and vulnerabilities*
> *opened up by rapid digitisation.*

Uttalelsen har i høyeste grad blitt aktuell fra mars 2019 når vi alle, de to siste årene, har vært med på «ekstremsport-uker» med tanke digitalisering i samfunnet grunnet pandemien.

5.6 Beslutningsteorier fra studien til Barth og de Jong

I teorikapittelet ble metodikken for å redusere fra 35 ulike beslutningsteoriene til 2 beslutningsteorier fra litteraturstudiet til Barth og de Jong (Barth og de Jong, 2017) beskrevet. Under vil jeg drøfte min beslutningsvei som endte opp med bruk av beslutningsteoriene om *planlagt atferd* og *rasjonell uvitenhet*.

Etter de to første silingsrundene var status at jeg var på 16 mulige beslutningsteorier som kunne være relevante for oppgaven. For å redusere ytterligere var jeg nødt til å dykke dypere ned i undersøkelsesmaterialet. Jeg analyserte hver tilbakemelding, på de enkelte spørsmålene fra den enkelte informant. Tilbakemeldingene koblet jeg opp mot det jeg mente var beste teori for akkurat denne tilbakemeldingen. Ganske tidlig utkrystalliserte det seg tre teorier som virket mer relevante enn de andre; teorien om *rasjonell uvitenhet*, *rasjonelle valg* og *planlagt atferd*. Alle disse tre beslutningsteoriene befant seg innenfor Barth og de Jongs undergruppe for *Rasjonell beregning av risiko og nytte* (Barth og de Jong, 2017) (se markering i figur 2.1). Tabellen under presenterer de ulike antall treff informantene fikk når jeg koblet deres tilbakemeldinger opp mot potensielt relevant teori.

Spørsmål – forkortet tekst	Beslutningsteorier: Rasjonell beregning av risiko og nytte (ref. figur 2.1) (Barth og de Jong, 2017)			Andre teorier	Ikke relevant
	Rasjonelle valg	Rasjonell uvitenhet	Planlagt atferd		
3 – Leste brukervilkår/ personvern-erklæring?		5	1		
4 – Forenklet pålogging	4				2
5 – Vurdering av helseopplysninger		6			
6 – Synkronisering med 3. part		1	1	2 *	2
7 – Profilering basert på smartklokkedata	2	1	3		
8 – beste/verste scenario	2	4			
9 – Verdi av helseopplysninger		6			
10 – Evaluering etterpå	2	1	3		
Sum	**10**	**24**	**8**	**2***	**4**
*Duality of Gemainschaft und Gesellschaft					

Tabell 5.1: Informantenes tilbakemeldinger på de enkelte spørsmålene koblet opp mot teori

Av overliggende tabell ser man at det er teorien om *rasjonell uvitenhet* som er mest relevant med 24 ulike treff, teorien om *rasjonelle valg* har 10 ulike treff, mens teorien om *planlagt atferd* har 8. I to av tilfellene var ikke spørsmålene relevante for informantene. Det skyldes at de ikke benyttet seg av eller ikke hadde anledning til å benytte forenklet pålogging, samt at de ikke synkroniserte med 3. parter. I tillegg var det 2 av treffene som gikk på teori innenfor Barth og de Jongs undergruppe, *Verdien av ønskede mål oppveier vurdert risiko (2a)* (Barth og de Jong, 2017). På grunn av lavt antall treff, velger jeg å utelate denne teorien og ønsker å fokusere der hovedtyngden av teoriene ligger.

For å kontrollere om de tre valgte teoriene syntes å være plausibel tolkning for denne oppgaven, hentet jeg frem refleksjonsnotatene etter både intervju og transkribering. Basert på en kombinasjon av:

- Hvilke beslutningsteorier jeg allerede hadde koblet aktuell tilbakemelding og informant opp mot og dens antall treff i aktuell teori.

- Hvilke(n) beslutningsteori(er) ville jeg ha koblet informanten opp mot basert på refleksjonsnotatene.

Kombinasjonen ga følgende resultater:

Informant-nummer	Beslutningsteorier: Rasjonell beregning av risiko og nytte (ref. figur 2.1) (Barth og de Jong, 2017)			Andre teorier	Ikke relevan	Vurdert teori koblet opp mot informanten
	Rasjonelle valg	Rasjonell uvitenhet	Planlagt atferd			
Informant 1	2	3	2		1	Planlagt atferd
Informant 2	2	3	2		1	Planlagt atferd
Informant 3	2	5		1*		Rasjonell uvitenhet
Informant 4	1	4	1		2	Rasjonell vurdering av personopplysninger + Planlagt atferd
Informant 5	1	5	1	1*		Rasjonell uvitenhet + Rasjonell utveksling av ressurser
Informant 6	2	4	2			Rasjonell uvitenhet + Planlagt atferd
Sum	**10**	**24**	**8**	**2***	**4**	
*Duality of Gemainschaft und Gesellschaft						

Tabell 5.2: Vurdert teori koblet opp mot informanten.

Markeringen i tabell 5.2 viser at teorien om *rasjonelle valg* ikke er den som synes å kunne forklare best data fra informantene som en helhet. På bakgrunn av analysen, mener jeg at teoriene om *planlagt atferd* og *rasjonell uvitenhet* er de to beslutningsteoriene fra litteraturstudiet til Barth og de Jong (Barth og de Jong, 2017) som best speiler informantenes vurderinger knyttet til bruksverdien av smartklokkedataene.

5.7 Oppsummering av funn i forhold til forventingene

Som forventet brydde informantene seg lite om brukervilkår og personvernerklæringer. Imidlertid var de svært bevisste på å ikke benytte seg av forenklet pålogging ved bruk av for eksempel Facebook- eller Google-konto. Dog innrømmet noen at de hadde benyttet forenklet pålogging fordi man satt med en følelse av hastverk – men det var innenfor andre kontekster. I tillegg var alle konsekvente med at de opprettet egne brukerkontoer (i motsetning til pålogging via en 3. part som f.eks. Facebook) i forbindelse med bruk av smartklokken.

Det som var et overraskende funn, var at ingen av informantene kunne tenke seg negative scenarioer knyttet til bruk av deres helseopplysninger utover de etiske dilemmaer som medfører hvis forsikringsselskapene får tak i disse opplysningene. Men også dette scenario er ikke sett som utelukkende negativt siden smartklokkedata kan gjøre det mulig å oppdage sykdom man foreløpig ikke merker selv, samt muligheter for rabattordninger. På den gode siden kom flere innspill som analysering av hjertefrekvens, bruk av fallsensor med mulighet for varsling, samt forskning. Imidlertid kom det tydelig frem i studien at informantene har et sterkere forhold til sine GPS-data kontra helseopplysninger. Med få utfordrende scenarioer hvor helseopplysninger kan misbrukes, var det heller ingen som klarte å sette noen konkret verdi på egne helseopplysninger. De så egentlig ingen grunn til å gjøre det, da flere uttrykket en «*jeg har intet å skjule*»-holdning, jf. diskusjon om funn fra Udoh og Alkharashi (Udoh og Alkharashi, 2016) ovenfor. Bakgrunnen for at jeg synes dette var et overraskende funn, er at den profesjonelle delen av hverdagen til alle informantene i stor grad handler om programvare som skal ivareta sensitive personopplysninger.

Teoriene jeg jobbet med, nemlig *planlagt atferd, rasjonell uvitenhet* og *beskyttende motivasjon*, ga alle – i kombinasjon eller alene – støtte til de tilbakemeldinger som informantene ga. Imidlertid deler jeg Williams, Nurse og Creese sitt syn om at teorien om *beskyttende motivasjon* passer godt innenfor personvern, da man får støtte gjennom å vurdere komponenter som appellerer til frykt og balansering mellom vurdering av alvorlighetsgrad, eksponering og mestringstro før en eventuell beskyttelsesmotivasjon vekkes. Det er også denne teorien som best støtter opp under tillit til håndtering av ens data, bruksverdien og endring av atferd.

Personvernparadokset, jeg må konkludere med at jeg ikke finner noe paradoks i forhold til informantenes bruk av smartklokken og de sensitive helseopplysningene. De har full tillit til sin samhandlingsaktør og er ikke bekymret for eventuell misbruk av helseopplysningene. Derimot er ikke informantene komfortable med at andre kan få kjennskap til deres GPS-data. Paradokset her er i så fall at GPS-data ikke er definert som sensitive personopplysninger, noe helseopplysningene er.

Min konklusjon for oppgaven følger derfor Solove's tanker; «*Personvernparadokset er en myte*» (Solove, 2021). Jeg deler oppfattelsen om at vi ikke kan ta enkeltbeslutninger som tas i spesifikke kontekster og overføre disse for å speile vår generelle holdning til personvern. Bruken av smartklokken er en liten del av informantenes hverdag. Jeg kan derfor ikke

definere deres holdning til personvern utelukkende basert på deres vurderinger knyttet til smartklokkens generering av helseopplysninger.

5.8 Oppsummering

I dette drøftings-kapittelet gjennomgikk jeg først sammenligning opp mot relevante studier. Videre drøftet jeg temaene personverninnstillinger, tillit til håndtering av mine data, dataenes verdi, potensiell endring i atferd, samt personvernparadokset. Som en avslutning diskuterer jeg valg av teorier, samt at jeg henter frem forventninger til funnene og koblet disse opp mot de faktiske funnene og konkluderer.

6. Konklusjon og veien videre

6.1 Konklusjon

Bakgrunnen for studiet ligger i et ønske om å forstå hvorfor vi deler så mye informasjon om oss selv via våre smartklokker. Deler av informasjonen er helseopplysninger som også er definert som sensitive data. Imidlertid har ikke disse dataene samme skjerming som helse-opplysninger som forvaltes innenfor helsesektoren. Formålet med studien er derfor å forstå:

> ***Hvilke vurderinger gjør smartklokkebrukere om bruksverdien til de sensitive persondata som ens smartklokke genererer?***

Gjennom intervjuer, metodearbeid, presentasjon av funn og drøfting har jeg forsøkt å besvare problemstillingen. Ved å sammenligne egne funn opp mot relevante studier finner jeg både fellestrekk og ulikheter. Fellestrekket var i hovedsak «*intet å skjule*»-holdningen, mens ulikheten besto i at det ikke eksisterer noe personvernparadoks for disse informantene innenfor denne konteksten. Informantene har gått til innkjøp av en smartklokke som de vil benytte til ønsket formål og bryr seg lite om de brukervilkår og personvernerklæringer som finnes. Aksept av vilkårene er bare et uhensiktsmessig steg på veien for å benytte smart-klokken. Derimot gjør informantene aktive vurderinger når det kommer til de videre spørsmålene som tilligger en installasjon- og registreringsprosess. Videre oppretter de egne brukerkontoer for formålet, samt at de aldri logger seg på hos smartklokkeprodusenten eller 3. parten, Strava, med Facebook- eller Google-konto.

Samtidig har informantene stor tillit til smartklokkeprodusentene og Strava når det gjelder håndtering av data. Selv om de vet at aktørene sitter på enorme mengder data som kan sammenstilles, er det ingen som har noen scenarioer som virkelig utfordrer når det gjelder misbruk av helseopplysningene som genereres av smartklokken. Derimot kommer det flere relevante scenarioer som gjelder misbruk av smartklokkens GPS-data, men som er utenfor omfanget av denne oppgaven da disse dataene ikke er å anse som sensitive. Som forventet var det ingen av informantene som klarte å sette en konkret verdi på egne helseopplysninger. Selv om det jobbes fra OECD sin side for å avklare dataenes verdi for å redusere ubalansen mellom de store aktørene og forbrukerne, har vi pr. i dag ingen kultur for å ta oss betalt for de data vi avgir.

For informantene er smartklokken i hovedgrunn et gode og et nyttig verktøy som bidrar til både motivasjon og inspirasjon for mer trening og bedre helse. Fordelene med de data som

genereres av smartklokkene er viktigere for informantene og oppveier de eventuelle ulempene som måtte finnes i forhold til aktørenes datainnsamling og viderebruk. All den tid informantene ikke er bekymret, har full tillit til aktørene og parallelt ikke kan se bruksverdien av sine sensitive helseopplysninger, konkluderer jeg med personvernparadokset ikke eksisterer blant mine informanter innenfor denne konteksten.

Imidlertid er det relevant å sitere igjen Buttarelli (Buttarelli, 2018): «*At dagens personvernparadoks henger sammen med at vi ennå ikke har lært hvordan vi skal navigere blant nye muligheter og sårbarheter som åpnes opp ved hurtig digitalisering*».

6.2 Studiens begrensninger

Som tidligere nevnt baserer jeg bacheloroppgaven på intervjuer fra seks informanter og hvor disse er mine kollegaer. Samtidig endte jeg opp med et relativt smalt aldersspenn blant informantene. Gjennom forskningsdesignet er det søkt tiltak for å redusere intervjueffekten som vil oppstå all den tid både informantene og jeg har en relasjon. Likevel er relasjonen og det smale aldersspennet en svakhet ved studiet.

6.3 Videre forskning

En videreutvikling av denne oppgaven kan være knyttet til en potensiell *ny definisjon av personvernparadokset* – det at vi ennå ikke har lært å navigere blant nye muligheter og sårbarheter. I denne studien har jeg begrenset meg til bruk av smartklokker i forhold til helseopplysninger. En smartklokke har ytterligere muligheter knyttet til helse. Det finnes blant annet mulighet til å lagre medisiner og dens doseringer, ta blodtrykk og hvor disse to eksemplene er sammenlignbare med hva som lagres av informasjon innenfor helsesektoren. I tillegg forventes stadig ny funksjonalitet all den tid helseopplysninger er interessant for de store aktørene. På den ene siden vil ny funksjonalitet gi oss bedre verktøy for å forvalte egen helse. Samtidig, på den andre siden kommer man ikke unna at de store aktørene fortsetter å akkumulere et stort volum av helseopplysninger. Det kunne vært interessant å forske på hvordan markedsmekanismer fungerer innenfor helseopplysninger og hvorfor dette antas å være en så stor forretningsmulighet for de største aktørene.

I tillegg viser studien en utbredt «*jeg har intet å skjule*»-holdning og derfor oppfattes ikke helseopplysningene til å være til skade for en selv, hverken i dag eller i morgen. Det som er litt forunderlig, er at de samme informantene har skjerming av personopplysninger som en integrert del av jobben. Men selvfølgelig, kontekst er viktig. De færreste er i dialog med helsesektoren fordi de velger det selv. Enkeltindividers dialog med helsesektoren skyldes ofte

et helsemessig problem man har behov for en løsning på. Derimot, bruk av smartklokker som middel for motivasjon og bedre helse – er et fritt valg og kan ha forebyggende helseeffekter på samfunnsnivå. Imidlertid, helseopplysninger er fremdeles helseopplysninger uavhengig hvordan de oppstår. Er det slik at helseopplysninger vi genererer selv er mindre verdt? Dette kunne også vært interessant å forske videre på.

Om jeg ikke skulle startet helt på bunnen med en ny oppgave, ville jeg utvidet omfanget på oppgaven til å inkludere smarttelefoner som kontrollgruppe. Smarttelefonene begynner å få svært avanserte funksjoner knyttet til helsen vår og hvor jeg antar at dataene ikke bare blir lagret lokalt på smarttelefonen, men også synkronisert til aktuell mobilprodusent.

Det er mange interessante tråder som trigges når det gjelder tillatelser til våre egne helseopplysninger og personvern. Vi er privilegerte som bor i et land hvor de fleste ikke har tradisjon og erfaring for å tenke scenarioer hvor data kan misbrukes. Samtidig er vi kanskje naive i vår tro på andres nytte av ens egne data?

7. Litteraturliste

Ajzen, I. (1991) The theory of planned behavior, *Organizational behavior and human decision processes*, 50(2), s. 179-211. doi: 10.1016/0749-5978(91)90020-T.

Anderssen, H. (2019) *Smartforsikringer: Flere kan få helseforsikring med ny teknologi*. Tilgjengelig fra: https://www.healthtalk.no/alle-artikler/helseforsikring-med-ny-teknologi/ (Hentet: 14/5- 2022).

Barnes, S. B. (2006) A privacy paradox: Social networking in the United States, *First Monday*, 11(9), s. 5. doi: 10.5210/fm.v11i9.1394.

Barth, S. og de Jong, M. D. T. (2017) The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, *Telematics and informatics*, 34(7), s. 1038-1058. doi: 10.1016/j.tele.2017.04.013.

Bergsjø, L. O. og Bergsjø, H. (2019) *Digital etikk : big data, algoritmer og kunstig intelligens*. Oslo: Universitetsforlaget.

Brown, B. (2001) Studying the Internet Experience, *HEWLETTPACKARD*. Tilgjengelig fra: https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.

Buttarelli, G. (2018) *40th ICDPPC: Opening Speech - Choose Humanity: Putting Dignity Back into Digital*. Tilgjengelig fra: https://edpl.lexxion.eu/data/article/13557/pdf/edpl_2018_04-026.pdf (Hentet: 26/3- 2022).

Carbonneau, S. (2021) *The Privacy Paradox: What Happens When Data Sharing is the Default*. Tilgjengelig fra: https://www.extendedmind.io/the-extended-mind-blog/the-privacy-paradox-what-happens-when-data-sharing-is-the-default (Hentet: 26/3- 2022).

Dahl, S. J. (2022) *Trender og status for personvernet 2022* (Hentet: 26/4 2022).

Datatilsynet (2013) *Big Data - personvernprinsipper under press*. Datatilsynet.no. Tilgjengelig fra: https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/big-data_web.pdf (Hentet: 31/1-2022).

Datatilsynet (2019) *Hva er en personopplysning?* Tilgjengelig fra: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/ (Hentet: 22/3- 2022).

Digitaliseringsdirektoratet (u.å.) *Hva er Schrems II-dommen?* Tilgjengelig fra: https://www.digdir.no/handlingsplanen/hva-er-schrems-ii-dommen/2581 (Hentet: 19/4- 2022).

Direktoratet for e-helse (2020) *Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren*. Tilgjengelig fra: https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren (Hentet: 14/4- 2022).

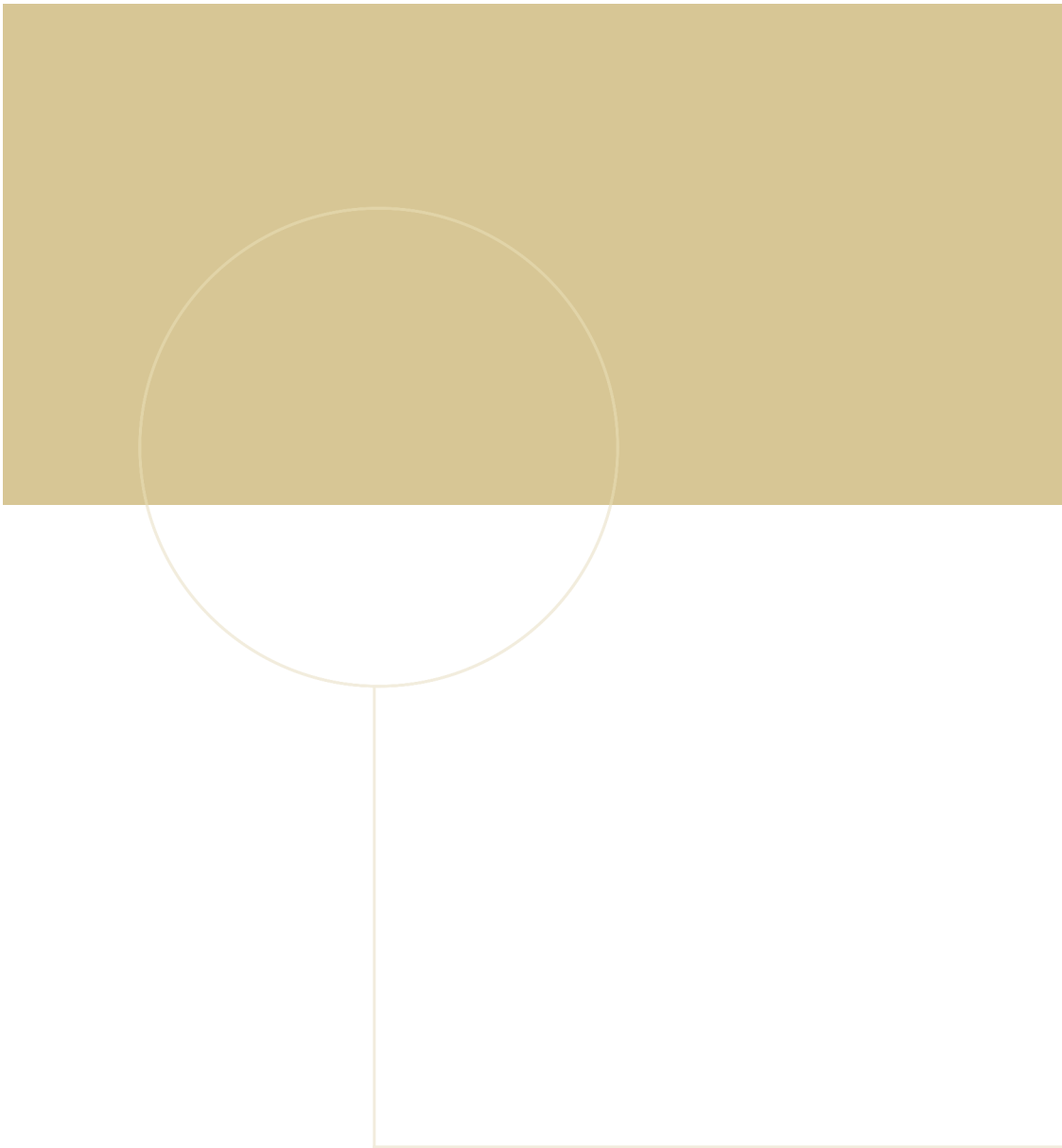
Downs, A. (1957) An Economic Theory of Political Action in a Democracy, *The Journal of political economy*, 65(2), s. 135-150. doi: 10.1086/257897.

EU (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. Tilgjengelig fra: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Hentet: 26/3- 2022).

Floyd, D. L., Prentice-Dunn, S. og Rogers, R. W. (2000) A Meta-Analysis of Research on Protection Motivation Theory, *Journal of applied social psychology*, 30(2), s. 407-429. doi: 10.1111/j.1559-1816.2000.tb02323.x.

Hughes-Roberts, T. (2015) Privacy as a secondary goal problem: an experiment examining control, *Information and computer security*, 23(4), s. 382-393.

Jacobsen, D. I. (2018) *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. CAPPELEN DAMM AS.
Johannessen, A., Christoffersen, L. og Tufte, P. A. (2011) *Forskningsmetode for økonomisk-administrative fag*. 3. utg. utg. Oslo: Abstrakt forl.
Ker, A. D. (2020) *Decoding the Privacy Paradox*. Tilgjengelig fra: https://theprivacyissue.com/privacy-and-society/decoding-privacy-paradox (Hentet: 22/3- 2022).
Lied, H. og Svendsen, C. (2018) *Slik røper soldater fra Norge, Danmark og USA hvem de er og hvor de trener i krigssoner*. Tilgjengelig fra: https://www.nrk.no/urix/slik-roper-soldater-fra-norge_-danmark-og-usa-hvem-de-er-og-hvor-de-trener-i-krigssoner-1.13891513 (Hentet: 3/4- 2022).
Lovdata (2018a) *Artikkel 9. Behanding av særlige kategorier av personopplysninger*. Tilgjengelig fra: https://lovdata.no/lov/2018-06-15-38/gdpr/a9 (Hentet: 22/3- 2022).
Lovdata (2018b) *Lov om behandling av personopplysninger (personopplysningsloven)*. Tilgjengelig fra: https://lovdata.no/lov/2018-06-15-38/gdpr/a22 (Hentet: 3/3- 2022).
Norberg, P. A., Horne, D. R. og Horne, D. A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, *Journal of Consumer Affairs*, 41(1), s. 100-126. doi: 10.1111/j.1745-6606.2006.00070.x.
Norsk helsenett (2022) *Hva er Helsenettet?* Tilgjengelig fra: https://www.nhn.no/helsenettet/hva-er-helsenettet (Hentet: 9/4- 2022).
Norton (2021) *The privacy paradox: How much privacy are we willing to give up online?* Tilgjengelig fra: https://us.norton.com/internetsecurity-privacy-how-much-privacy-we-give-up.html (Hentet: 22/3- 2022).
Rogers, R. W. (1975) A protection motivation theory of fear appeals and attitude change, *The journal of psychology*, 91(1), s. 93.
Solove, D. J. (2021) The myth of the privacy paradox, *Geo. Wash. L. Rev.*, 89, s. 1. Tilgjengelig fra: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2738&context=faculty_publications (Hentet: 26/3-2022).
Strava (2022) *INSPIRE YOUR ATHLETES - Sports are about more than working out — they're about community.* Tilgjengelig fra: https://business.strava.com/ (Hentet: 3/4-2022).
Udoh, E. S. og Alkharashi, A. (2016) Privacy Risk Awareness and the Behavior of Smartwatch Users: A Case Study of Indiana University Students, i *Future Technologies Conference (FTC), San Francisco, CA, Dec 06-07*. NEW YORK: IEEE, s. 926-931.
Williams, M., Nurse, J. R. C. og Creese, S. (2019) Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study, *Computers in Human Behavior*, 99, s. 38-54. doi: 10.1016/j.chb.2019.04.026.



NTNU

Norwegian University of
Science and Technology