LUNDS UNIVERSITET
Ekonomihögskolan
Institutionen för informatik

Integritet i rörelse

En studie av användarens avvägning mellan fördelar och risker i samband med datadelning i träningsapplikationer

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: John Ljungqvist
Daniel Åbjörnsson

Handledare: Christina Keller

Rättande lärare: Nicklas Holmberg
Miranda Kajtazi

Integritet i rörelse: En studie av användarens avvägning mellan fördelar och risker i samband med datadelning i träningsapplikationer

ENGELSK TITEL: Privacy in motion: A study of the user's trade-off between benefits and risks in connection with data sharing in fitness applications

FÖRFATTARE: John Ljungqvist, Daniel Åbjörnsson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: maj, 2024

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 49

NYCKELORD: Träningsapplikationer, Privacy Calculus Theory, Integritetsrisker, Dataskydd, Användare

SAMMANFATTNING (MAX. 200 ORD): Denna studie utforskar hur upplevd risk och upplevt värde påverkar användares intention att dela data med träningsapplikationer. Genom enkätundersökningar riktade till användare i Sverige, ger studien insikter i hur användarna gör avvägningar mellan risker och fördelar enligt Privacy Calculus Theory. Under perioden 2020 till 2023 ökade användningen av träningsapplikationer markant, samtidigt som medvetenheten om integritetsrisker också steg. Resultaten visar att även om användare generellt känner oro för integritetsintrång, är de villiga att dela sin information om de upplever att fördelarna överväger riskerna. Studien bekräftar, som i tidigare forskning att demografiska faktorer som ålder och kön påverkar hur individer värderar dessa risker och fördelar. Äldre och kvinnor visar sig vara mer riskmedvetna och försiktiga.

Innehåll

Figurer

Tabeller

1 Introduktion

1.1 Bakgrund

Under perioden 2020 till 2023 ökade antalet användare av träningsapplikationer på marknaden från 98 miljoner till 162 miljoner, vilket motsvarar en ökning på cirka 66 % (Statista, 2024). Parallellt uttryckte 64 % av svenskarna oro över den ökande insamlingen och användningen av personlig information i samhället, enligt en undersökning utförd av Insight Intelligence (2018). Brough och Martin (2020) belyser hur COVID-19-pandemin har ökat påverkan på vår integritet genom att göra oss mer sårbara när vi delar känslig information online. Den ökade användningen av digitala tjänster under pandemin innebär att vi delar mer personlig och känslig information, vilket minskar skyddet och utsätter oss för nya risker. Detta scenario har minskat individers kontroll över deras data men också ökat medvetenheten om riskerna med datadelning och potentiella brott mot integriteten.

Träningsapplikationer använder data som samlas in från telefonens inbyggda verktyg, såsom GPS, accelerometer, mikrofon, högtalare, och kamera, för att mäta hälsoparametrar. Dessa verktyg möjliggör för applikationerna att samla in och analysera information relaterad till fysisk aktivitet, såsom löpsträckor, hastighet, antal steg, och även användarens plats under träningspasset. Grundläggande personlig information såsom namn, ålder, och kön, tillsammans med hälsorelaterade data som kroppsmått och träningsnivå, möjliggör för applikationerna att skapa personliga träningsplaner och målsättningar (Higgins, 2016). Många träningsapplikationer interagerar med bärbara enheter såsom träningsklockor och pulsmätare för att samla in biometrisk data som hjärtfrekvens och sömnkvalitet, vilket ger ytterligare insikter i användarens hälsostatus. Mat- och näringsuppgifter hjälper användare att övervaka sitt kaloriintag och näringsinnehåll. Användarbeteende inom applikationerna ger viktig information för att ytterligare personalisera upplevelsen och förbättra tjänsten (Bajpai et al., 2015).

Enligt Brakemeier et al. (2016) påverkar individers målinriktning att sträva efter att uppnå positiva resultat eller att undvika negativa utfall samt hur de bedömer risker och fördelar när de delar personlig information. När en person upplever höga risker, tenderar denne att prioritera att undvika dessa risker, vilket gör att fördelarna tycks mindre betydelsefulla i beslutsprocessen. Denna förståelse av hur människor beslutar om sin datadelning stöds även av Privacy Calculus Theory, som visar att beslut att dela personlig data ofta baseras på en avvägning mellan upplevd risk och upplevt värde (is.theorizeit.org, n.d.).

Med införandet av dataskyddsförordningen (GDPR), har Europeiska unionen etablerat en av de strängaste dataskyddslagstiftningarna i världen. GDPR syftar till att ge individer större kontroll över sina personuppgifter, samtidigt som det inför skärpta krav på organisationer som behandlar data (Integritetsskyddsmyndigheten, 2024). För utvecklare av träningsapplikationer innebär detta en rad viktiga skyldigheter, särskilt med tanke på de känsliga personuppgifter som dessa applikationer ofta hanterar. Känsliga personuppgifter, enligt GDPR, inkluderar data som avslöjar ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska

övertygelser, eller medlemskap i fackföreningar, samt genetiska och biometriska data för att entydigt identifiera en individ, data om hälsa eller data om en persons sexualliv eller sexuell läggning (Integritetsskyddsmyndigheten, 2021). Inom kontexten av träningsapplikationer sträcker sig känsliga personuppgifter ofta till data om hälsa, såsom hjärtfrekvens, sömnkvalitet, fysisk aktivitetsfrekvens, och detaljerad träningsstatistik. Dessa uppgifter kan potentiellt avslöja information om användarens fysiska hälsotillstånd och livsstil, vilket gör dem till känsliga personuppgifter enligt definitionen i GDPR. Företag som utvecklar träningsapplikationer måste därför vidta specifika åtgärder för att skydda användarens personuppgifter. Detta omfattar att säkerställa att processerna för datainsamling, -lagring och -behandling är utformade för att bevara datasekretessen (Integritetsskyddsmyndigheten, 2021).

Shah et. al (2019) framhåller att viktiga åtgärder innefattar kravet på att inhämta samtycke från användaren före någon form av insamling eller bearbetning av känsliga personuppgifter. Det krävs också att användaren informeras om hur deras data kommer att användas, var den lagras och hur den skyddas. Företagen är även skyldiga att tillhandahålla användaren möjligheter att enkelt få tillgång till, korrigera felaktigheter i, och begära radering av sina personuppgifter. Följaktligen tvingas många företag genomföra omfattande förändringar i sina datasystem för att uppfylla kraven i GDPR. Utmaningarna med de befintliga systemen hos företag är att dessa måste uppgraderas för att vara GDPR-kompatibla. GDPR är avsedd att skydda personuppgifter för alla som bor inom EU. Följaktligen är företag som har kunder från EU juridiskt förpliktade att följa dessa regler (Shah et al. 2019).

1.2 Problemområde

Smarta telefoner är utrustade med funktioner som kan tillåta oönskade parter att övervaka användaren. Sådana parter kan missbruka telefonens kamera, mikrofon eller GPS för att övervaka användarens aktiviteter. Ironiskt nog leder tillägget av fler avancerade funktioner i dessa enheter också till ökad sårbarhet för säkerhetsintrång. Detta gör enheterna till ett attraktivt mål för cyberbrottslingar. Trots att företag formulerar integritetspolicyer, sker dataöverföringar ofta okrypterade över oskyddade nätverk, vilket komprometterar användarnas information (Bui, 2016).

Marknadens expansion medför ökade utmaningar i att skydda användarens information. General Data Protection Regulation (GDPR), som trädde i kraft inom Europeiska unionen år 2018, spelar en avgörande roll i skyddet av datasekretess och etik. Denna lagstiftning syftar till att stärka och harmonisera dataskyddet för individer inom EU och inför strikta regler för företags insamling, lagring och hantering av personuppgifter (Integritetsskyddsmyndigheten, 2021). För applikationer inom träningssektorn utgör detta en särskild utmaning på grund av den ofta känsliga naturen hos den insamlade personliga informationen. För att upprätthålla användarens förtroende och efterleva lagstiftningen krävs höga säkerhetsstandarder och transparent kommunikation om dataanvändning (Stach 2018).

Under 2023 registrerades 10 276 anmälningar om dataintrång i Sverige, vilket markerar en ökning från de 8 993 anmälningar som dokumenterades under 2022 (säkerhetskollen.se, nd.), Cirka hälften av dessa dataintrång under 2023 kan hänföras till sociala medier eller elektroniska tjänster, medan 15 % involverade olovlig registerslagning. Ytterligare 3 % av fallen var relaterade till överbelastningsattacker och skadlig kod använd i utpressningssyfte, medan de resterande 33 % av fallen klassificerades som andra former av dataintrång.

Digitaliseringen av samhället medför många möjligheter, med leder också till ökade sårbarheter. Därför blir integritet och datasäkerhet alltmer centrala. Det är avgörande att implementera förbättrade säkerhetsåtgärder och förstärka transparensen i datahanteringen för att skydda användarnas personliga information och upprätthålla förtroendet för digitala plattformar (Lindskog et al., 2022).

Hamed och Ayed (2016) diskuterar problematiken kring datainsamling i applikationer och användarnas brist på medvetenhet. De belyser hur denna brist på transparens direkt försvagar användarnas personliga integritet och förtroende genom att personlig information ofta samlas in och överförs till tredje part utan uttryckligt samtycke. Hamed och Ayed (2016) argumenterar för att denna oönskade datainsamling och dess delning med tredje part kan resultera i flera negativa konsekvenser för användaren. Dessa inkluderar, men är inte begränsade till, målinriktad reklam baserad på personlig information och mer allvarliga risker såsom övervakning. Bhatia och Breaux (2018) diskuterar också problemen kring hur personlig information samlas in och används av företag. De framhäver att trots att individers upplevelse av integritetsrisker kan mätas och kvantifieras genom empiriska metoder, så kvarstår betydande risker när det gäller att skydda personlig integritet i digitala miljöer. Författarna pekar på att även om individer kan vara mer benägna att dela sin information när de upplever fördelarna med att dela som större än riskerna, innebär detta inte att integritetsriskerna är eliminerade. I stället exponeras användare för en rad integritetsintrång där deras data kan missbrukas för målinriktad reklam eller övervakning, ofta utan deras medvetna samtycke. Resultaten av forskningen pekar på en betydande förlust av kontroll över den egna informationen, vilket direkt påverkar användarnas förtroende för och upplevelsen av digitala tjänster (Hamad & Ayed, 2016)

1.3 Forskningsfråga

Med bakgrund av problemområdet och dess avgränsningar ställer vi oss följande forskningsfråga:

Hur påverkar upplevd risk och upplevt värde, användares intention att dela data med träningsapplikationer?

1.4 Syfte

Det övergripande syftet med denna studie är att empiriskt utforska hur upplevd risk och upplevt värde påverkar användares intention att dela data med träningsapplikationer. För att uppnå detta syfte, kommer studien att fokusera på att samla in kvantitativa data genom en enkätundersökning riktad till användare av träningsapplikationer.

1.5 Avgränsningar

Forskningen kommer att avgränsas till att inkludera individer i Sverige, med ett fokus på applikationer som samlar in hälsorelaterad data inom fysisk träning. Denna data omfattar inte enbart grundläggande information såsom vikt, kön, ålder, hjärtfrekvens, och sömnkvalitet, utan sträcker sig även till mer detaljerade och känsliga personuppgifter. Dessa inkluderar,

men är inte begränsade till, specifika träningsstatistik, kostintag, stressnivåer, fysisk aktivitetsfrekvens, och eventuella hälsotillstånd som kan påverkas av eller påverka användarens träningsrutiner. Studien kommer att exkludera applikationer som primärt är avsedda för sjukvårdssektorn eller medicinsk användning, för att fokusera på de etiska och sekretessmässiga utmaningarna med anknytning till insamling av personuppgifter i träningsapplikationer.

2 Litteraturgenomgång

2.1 Dataskyddsförordningen (GDPR)

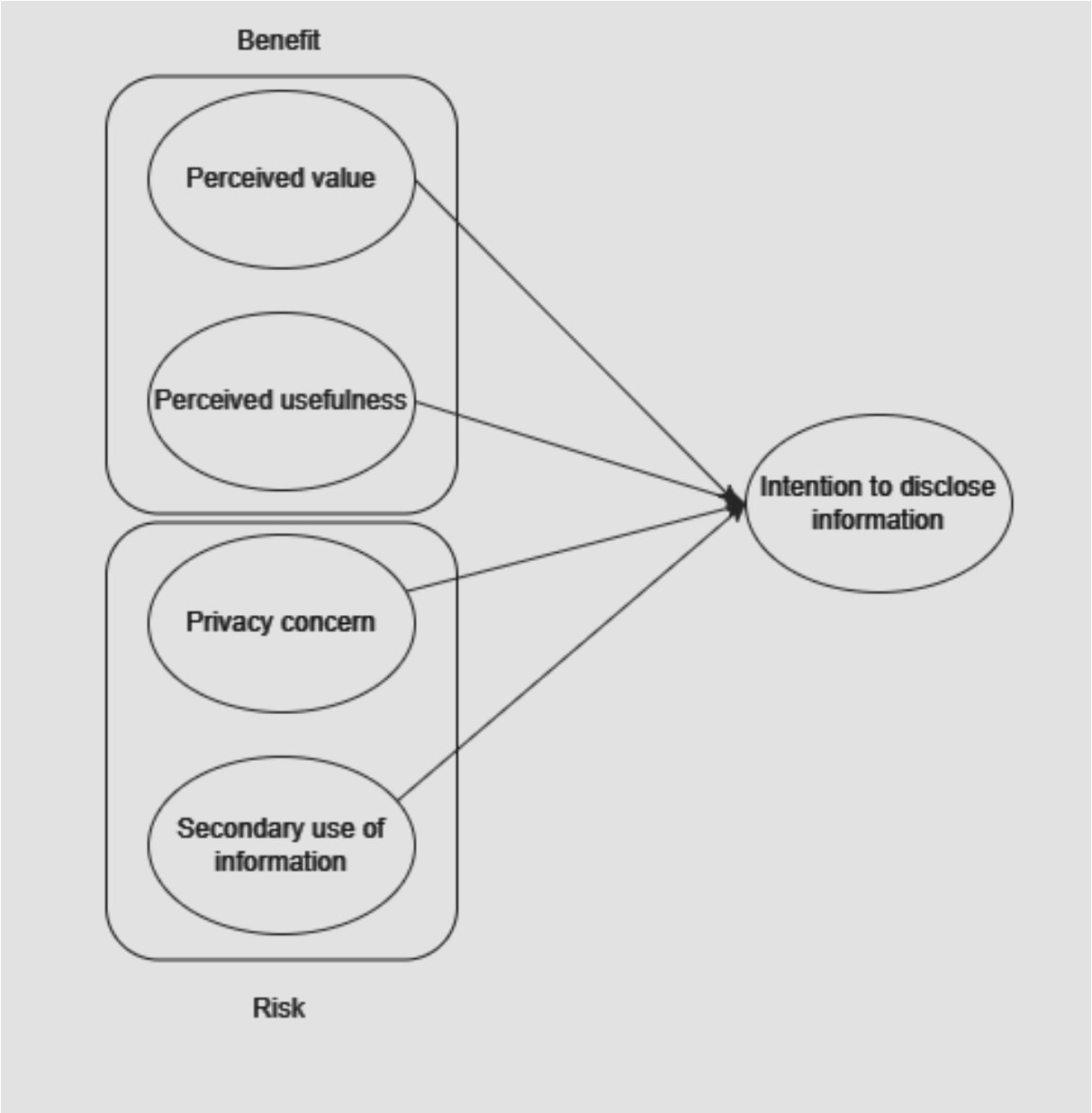
General Data Protection Regulation (GDPR) är en omfattande dataskyddsförordning som antogs av Europeiska unionen (EU) och började gälla den 25 maj 2018. Den ersatte det tidigare dataskyddsdirektivet från 1995 och syftar till att ge individer större kontroll över sina personuppgifter. GDPR ger strikta regler för hur organisationer får samla in, använda, och lagra personuppgifter. Direktivet omfattar alla typer av personuppgifter – allt från namn och hemadress till hälsouppgifter såsom längd och sömnmönster. Organisationer måste säkerställa att de har klart och tydligt samtycke från individen för att behandla deras personuppgifter, och det måste vara lika enkelt att dra tillbaka samtycket som det var att ge det. Dessutom ger GDPR individer flera rättigheter, inklusive rätten till tillgång, rätten till radering och rätten till dataportabilitet, vilket gör det möjligt för individer att ta med sig sina personuppgifter från en tjänst till en annan (Integritetsskyddsmyndigheten, 2021).

2.2 Privacy Calculus Theory

Den pågående digitaliseringen, som omfattar data, information, och diverse processer, integreras alltmer i våra liv, oberoende av om det berör arbets- eller privatlivet. En grundläggande förutsättning för implementeringen av smart teknologi är insamlandet och analysen av omfattande datamängder, vilket understryks i den befintliga litteraturen (Schomakers et al., 2021). En undersökning utförd av Europeiska kommissionen (2019) avslöjar att endast 14 % av Europas befolkning känner att de har full kontroll över sin personliga data. Även om det rapporteras om en låg andel som upplever kontroll över sin personliga data innebär det inte nödvändigtvis att man tar till åtgärder för att skydda sin data eller nekar till att utelämna information. Denna attityd benämns som “Privacy Paradox” och behandlas av Privacy Calculus Theory (Schomakers et al. 2021).

Privacy Calculus Theory (is.theorizeit.org, n.d.) är ett teoretiskt ramverk som används för att förstå hur individer gör avvägningar mellan upplevda fördelar och risker när de överväger att avslöja personlig information, särskilt i en digital eller mobil miljö. Teorin undersöker de underliggande mekanismerna som påverkar användarens avsikter att avslöja personlig information genom mobila applikationer. Enligt Privacy Calculus Theory är individers vilja att dela personlig information inte enbart beroende av deras oro för integritet, utan också av de upplevda positiva utfallen av att göra det. Det innebär att även om en individ kan vara orolig för sin personliga integritet, kan den samma individen fortfarande välja att dela personlig information om de upplevda fördelarna uppväger de upplevda riskerna (Cho et al., 2018)

Enligt Cho et al. (2018) är denna teori särskilt relevant i sammanhang där teknologi ställer användare inför avvägningar mellan integritetsrisker och upplevda fördelar, som till exempel förbättrad hälsostatus och träning. Denna forskning utvidgar förståelsen för hur olika motivationsfaktorer (se figur 2.1), som personlig träning och hälsoövervakning, bidrar till att upplevda fördelar ofta uppväger de potentiella riskerna, vilket är centralt i analysen av användarbeteenden i samband med integritet och datadelning Cho et al. (2018).



Figur 2.1: Privacy Calculus Theory (anpassad utifrån Cho et al., 2018)

Teorins diagram representerar hur individer väljer att dela eller inte dela personlig information online baserat på en avvägning mellan upplevda risker och fördelar. Teorin belyser den inre process som pågår när man överväger integritetsrisker kontra de potentiella fördelarna av att använda digitala tjänster (is.theorizeit.org, n.d.). Nedan följer en genomgång av de olika delarna i teorins diagram:

Perceived Value och Perceived Usefulness (Fördelar) – Individer bedömer värdet och användbarheten av att dela information. Dessa faktorer bidrar till de upplevda fördelarna av att dela med sig av personlig information. Om det ger fördelar, exempelvis i form av ökad bekvämlighet eller monetära fördelar och upplevs som stora, ökar sannolikheten att individer delar med sig av sin information (Majumdar & Bose, 2015).

Privacy Concern och Secondary Use of Information (Risker) – Integritetsoro hänvisar till den oro och de rädslor kopplat till delad information som kan missbrukas eller otillbörligen åtkommen. Sekundär användning av information hänvisar till användningen av data med

andra syften än det som var menat från början. Dessa faktorer är risker som kan avskräcka individer från att dela information (Knijnenburg et al., 2017).

Intention to Disclose Information - Begreppet "Intention att avslöja information" från Privacy Calculus Theory innebär att intentionen att avslöja information påverkas av en avvägning mellan upplevda fördelar och risker. Om fördelarna överväger riskerna ökar sannolikheten för att informationen avslöjas. Tvärtom, om riskerna uppfattas som större än fördelarna, minskar sannolikheten för att information ska avslöjas. Denna beslutsprocess påverkas av hur individer värderar sin integritet och nyttan av den tjänst eller produkt som är aktuell (Dinev & Hart, 2006).

2.3 Skydd av användardata

Skydd av användardata refererar till de strategier och metoder som implementeras i bland annat applikationer för att säkerställa integriteten, konfidentialiteten, och tillgängligheten av personlig information som samlas in, lagras och bearbetas. Denna process innefattar efterlevnad av relevanta lagar och regelverk, samt tillämpning av teknologier som kryptering och förebyggande av dataläckage för att förhindra obehörig åtkomst och garantera användarens datasekretess. Vikten av att skilja mellan dataskydd och datasekretess betonas, där det förstnämnda fokuserar på tekniska och administrativa åtgärder för att skydda data, medan det senare hanterar rättigheterna kring insamling och användning av personuppgifter (Cloudian, 2022).

I takt med att mobiltelefoner och andra smarta enheter blir en allt större del av våra liv, blir skyddet av personlig information allt viktigare. En nyckelfaktor för att skyddet ska kunna fungera är utformningen av applikationer, med särskilt fokus på användbarheten inom inställningarna för dataskydd. En studie av Chen et al. (2021) visar att många applikationer idag gör det möjligt för användare att anpassa sina inställningar för dataskydd, hela 80 %. Dock framkommer det att endast 40 % av applikationerna erbjuder tydlig information och kontrollmöjligheter för användaren att inaktivera platstjänster och andra tjänster som lagrar information.

Denna information är väsentlig eftersom den understryker hur viktigt det är med tydlighet och kontroll över vår data. För att skydda vår information och öka vårt förtroende för digitala tjänster, tyder Chen et al. (2021) på att applikationer måste göra det lätt för individen att förstå och ändra våra dataskyddsinställningar. Chen et al. (2021) påpekar också att även om säkerhetsåtgärder som kryptering är viktiga, är det också kritiskt att ha en design som är öppen och låter användare kontrollera sin information. Författarna vill öka behovet av att inkludera enkla dataskyddsinställningar i utvecklingen av applikationer. Genom att göra detta kan utvecklare följa lagar som GDPR och samtidigt bygga starkare relationer med sina användare genom att visa respekt för deras integritet. Skyddet av användardata handlar inte bara om teknik, utan också om hur användarvänlig den tekniken är.

I vår uppsats har vi valt att använda Privacy Calculus Theory i vår empiriska datainsamling, eftersom teorin ger en förståelse för hur till exempel träningsapplikationer, som ständigt samlar in och hanterar personuppgifter, kan påverka användarnas intention om datadelning.

2.4 Tidigare forskning kring användares delning av information i träningsapplikationer

Tidigare forskning inom ämnet integritet och dataskydd, med särskild inriktning på träningsapplikationer med tillhörande bärbar teknologi, har tagit upp flera viktiga aspekter när det kommer till problematiken inom datainsamling. Forskning som genomförts av Stach (2018) vid Universitetet i Stuttgart undersöker användningen av träningsapplikationer och hur dessa samlar in data. Stach (2018) framhäver särskilt integritetsproblem med träningsapplikationer som samlar in både hälsodata och personlig information, vilket resulterar i en detaljerad översikt över användarens livsstil och vanor genom användningen av sådan information. Han påpekar att många av dessa applikationer kränker användarens integritet och missbrukar insamlad data. Särskilt lyfter Stach (2018) fram problematiken med applikationer som säljer insamlad data till tredje part, såsom försäkringsbolag eller annonsindustrin, utan användarens uttryckliga samtycke eller medvetenhet. Detta beteende innebär en betydande risk för användarens integritet, då det kan leda till oönskad exponering av känslig personlig och hälsorelaterad information.

Stach (2018) argumenterar för införandet av en Privacy Policy Model och en Privacy Management Platform som strategier i träningsapplikationer för att ge användaren större kontroll över deras data. Privacy Policy Model och Privacy Management Platform är två centrala koncept inom hantering av dataskydd och personlig integritet i organisationer (Mitschang and Stach, 2014). Medan Privacy Policy Model fokuserar på de riktlinjer och regler som en organisation utformar för att hantera och skydda personuppgifter, syftar Privacy Management Platform till att tekniskt stödja dessa processer. Genom att implementera dessa verktyg kan utvecklare av träningsapplikationer säkerställa att användardata hanteras på ett transparent och användarcentrerat sätt, där användarens integritet respekteras och skyddas. Det bidrar inte bara till att höja användarens tillit till applikationerna utan också till att främja en mer ansvarsfull användning av persondata inom applikationerna. Genom att implementera en Privacy Management Platform kan företag effektivisera efterlevnaden av dataskyddslagar, automatisera hantering av samtycken, och hantera användardata på ett säkert sätt. Mitschang och Stach (2014) framhåller att dessa två begrepp kompletterar varandra, där policy-modellen utgör ramverket för integritetshanteringen, medan plattformen tillhandahåller de verktyg som nödvändiga för att genomföra dessa policyer.

Zimmer et. al (2018) studerar användarens upplevelser och inställningar till integritetsfrågor kopplade till användningen av träningsklockor med tillhörande applikationer. Studiens syfte är att ge en mer komplett bild av hur användare av träningsklockor upplever dessa enheter och hur de hanterar sin personliga träningsinformation ur ett integritetsperspektiv. Forskarna använder sig av Communication Privacy Management som teoretiskt ramverk och presenterar resultat baserade på både enkät- och intervjudata om fördelarna och nackdelarna användarna upplever, samt hur integritetsproblem och beteenden kopplas till användarens strategier för att hantera integritetsgränser relaterade till personlig träningsinformation. Studien bidrar till framtida policyer för insamling av information relaterad till den växande användningen av bärbar teknik med tillhörande träningsapplikationer. Forskarna konstaterar att fördelarna med att använda träningsklockor upplevs som väsentligt större än nackdelarna. De mest framträdande fördelarna inkluderar motivation till ökad fysisk aktivitet, förbättrad sömnkvalitet och viktminskning. När det gäller integritetsproblemen uttrycker många deltagare en låg nivå av oro för hur deras personliga uppgifter hanteras. Majoriteten av deltagarna anser inte att informationen som samlas in av träningsapplikationer är tillräckligt känslig för att utgöra ett integritetsproblem. Dock uppstår vissa bekymmer när det gäller

potentialen för att denna information ska kunna samlas in och användas på sätt som deltagarna inte har förutsett eller gett sitt samtycke till, särskilt när det gäller delning av data med tredje part som försäkringsbolag eller i juridiska sammanhang (Zimmer et al., 2018).

Yang et al. (2016) undersöker användaracceptansen av bärbara enheter, med fokus på det upplevda värdet och hur det påverkar användarens avsikt att använda tekniken. I studien använder sig författarna av en egenutvecklad forskningsmodell för att analysera användarnas upplevda värde av bärbara enheter. Modellen fokuserar specifikt på hur olika komponenter av upplevd nytta, såsom användbarhet, nöje och social image, har en större inverkan på det upplevda värdet jämfört med upplevda risker. Deras forskning belyser hur funktionalitet och kompatibilitet direkt påverkar användarnas upplevda nytta, vilket i sin tur främjar teknikanvändning. Dessutom framhäver studien betydelsen av visuell attraktivitet och varumärkesimage, som starkt påverkar användarens emotionella engagemang och uppfattade nytta av enheten (Yang et al., 2016).

Yang et al. (2016) tar även upp riskuppfattningar som kan påverka användarnas benägenhet att använda bärbara teknologier. Studien framhäver två huvudsakliga risktyper, prestanda och finansiell risk som negativt påverkar det upplevda värdet och därmed användarnas acceptans. Denna aspekt är särskilt relevant i sammanhang där användare hanterar personlig och känslig information, exempelvis hälsodata som samlas in via träningsapplikationer.

Schomakers et al (2021) undersöker hur integritetsoro påverkar användares acceptans för smarta teknologier, exempelvis ”activity trackers” inom fitness. Studien undersöker individer i Tyskland. De applicerade Privacy Calculus Theory och fann att användarna identifierade fördelarna med aktivitetstrackers i form av övervakning av personlig hälsa och optimering av livsstil. Integritetsoron var huvudsakligen baserad på hur personlig information kan användas och risken för dataintrång. Studien understryker att viljan att dela personlig information och acceptera teknik är i första hand driven av en komplex avvägning mellan vad användarna kan tjäna på det och de potentiella riskerna.

Abdelhamid (2021) undersökte användare av fitnessapplikationer och hur de förhåller sig till integritet och hur detta påverkar viljan att dela med sig av personlig information. Målet med studien var att undersöka hur detaljerad kontroll påverkar användarens vilja att dela information. Förtroende för applikationen och upplevda risker påverkade avsevärt användarnas vilja att dela sina data. Högre förtroende och lägre upplevda risker relaterade till integritet ökade sannolikheten för datadelning. Användare som kände igen konkreta fördelar med att använda aktivitetsarmband, såsom förbättrad hälsokontroll och personlig återkoppling, var mer benägna att dela med sig av sina data. Att tillhandahålla användare med detaljerade integritetskontroller är avgörande för att uppmuntra fortsatt användning av aktivitetsarmband. Användare känner sig mer bekväma med att dela personlig information när de kan kontrollera vem som ser deras data och vilka data som delas.

2.5 Ålder, kön och användarfrekvens

Ålder är en betydande faktor i hur individer uppfattar och interagerar med risker, särskilt i användningen av digital teknologi såsom träningsapplikationer. Forskning visar att yngre användare ofta är mer benägna att dela personlig information online jämfört med äldre användare. Denna tendens kan förklaras genom en kombination av ökad teknisk förtrogenhet och en mindre utvecklad riskmedvetenhet bland yngre individer (Zeissig et al., 2017). Å andra

sidan tenderar äldre användare att vara mer försiktiga med att dela personlig information på grund av högre riskmedvetande och oro för sin integritet (Boise et al., 2013).

Enligt Privacy Calculus Theory, som vi baserar vår sambandsanalys på i senare kapitel, kan denna åldersrelaterade skillnad i beteende bero på en avvägning mellan upplevd nytta och upplevda risker (Zeissig et al., 2017). Äldre användare tenderar att inte se samma nytta av att dela sin data som yngre gör, vilket gör att deras riskbedömningar får större vikt i deras beslutsprocesser. Vidare kan erfarenheter från livet och en mer etablerad syn på privatliv bidra till en starkare känslighet för integritetsfrågor hos äldre individer (Zeissig et al., 2017).

Enligt Harris et al. (2006) uppvisar kvinnor och män betydande skillnader i hur de uppfattar och hanterar risker. Forskning visar att kvinnor tenderar att vara mer försiktiga och mindre benägna att engagera sig i riskfyllda beteenden. Kvinnor bedömer sannolikheten för negativa utfall högre och förväntar sig mindre positiva följder av riskfyllda aktiviteter, vilket bidrar till deras lägre benägenhet att engagera sig i risktagande inom olika områden (Harris et al., 2006). Däremot visar forskningen att även när det gäller positiva riskområden, där utfallen är osäkra men potentiellt gynnsamma, är kvinnor mer benägna att engagera sig. Detta fenomen kan delvis förklaras av att kvinnor generellt sett har en mer optimistisk bedömning av sannolikheten för positiva utfall (Harris et al., 2006). Eckel och Grossman (2008) tillägger att kvinnor inte bara är mer försiktiga, utan de är också generellt bättre på att bedöma risker än män.

Cho et al. (2018) använder Privacy Calculus Theory bland användare av bärbar teknologi, såsom smartklockor och pulsband, för att bedöma för- och nackdelar med att dela känslig hälso- och träningsinformation. Studien visar specifikt att de individer som tränar frekvent tenderar att uppleva mer fördelar med teknologin, vilket ökar deras vilja att dela med sig av personlig information. Det framgår att dessa användare, genom att ofta träna, får större nytta av anpassade hälsodata och träningsinsikter, vilket gör dem mer benägna att acceptera eventuella integritetsrisker. Resultaten pekar på att träningsfrekvensen signifikant påverkar hur fördelarna värderas i förhållande till de potentiella riskerna, vilket leder till att aktiva användare ofta väljer att dela sin information (Cho et al., 2018).

3 Metod

I metodkapitlet kommer vi att presentera valda metoder för vår undersökning, val av respondenter, insamling och analys av den empiriska datan. Vi kommer även att ta upp de etiska övervägandena som varit vägledande i studiens utförande samt de åtgärder som vidtagits för att säkerställa studiens validitet och reliabilitet.

3.1 Litteratursökning

För att hitta relevant tidigare forskning om Privacy Calculus Theory kopplat till träningsapplikationer har vi använt oss av flera databaser, däribland LUBSearch, IEEE Xplore, Semantic Scholar, Consensus och Google Scholar som hänvisar mycket av artiklarna till ScienceDirect. Härigenom har vi hittat ett brett utbud av vetenskapliga artiklar som vi har använt. Vi började vår litteratursökning med generella sökord som “fitness apps” och “privacy data” för att få en övergripande uppfattning om den befintliga forskningen. Efter vi fick väldigt många träffar på de sökorden, i snitt flera tusen på de olika plattformarna, behövde vi specificera vår sökning för att hitta mer relevant material. Vi ändrade och kombinerade därför våra söktermer med begrepp som “privacy calculus theory”, “information disclosure”, “wearable technology” och “privacy data protection”. Dessa riktade söktermer resulterade i färre och mer relevanta artiklar. På IEEE Xplore, Semantic Scholar, Consensus och ScienceDirect kunde vi även se antalet citeringar, vilket hjälpte oss ytterligare att identifiera relevanta artiklar.

Trots en bred genomgång av befintlig litteratur upptäckte vi att det inte finns någon exakt forskning som utforskar tillämpningen av Privacy Calculus Theory på träningsapplikationer över olika demografiska grupper. Även om vi inte fann denna specifika forskning, undersökte vi tidigare arbeten som rör olika aspekter av vårt forskningsområde, till exempel hur Privacy Calculus Theory har tillämpats i liknande sammanhang, såsom Cho et al. (2018) forskning om bärbara enheter kopplat till träning.

3.2 Metodval

I denna studie används en forskningsmetod som är influerad av kvantitativa metoder genom en enkätundersökning för att utforska hur datainsamling påverkar användares intention att dela data med träningsapplikationer. Studiens teoretiska ramverk är baserat på Privacy Calculus Theory, som förklarar avvägningen mellan personlig integritet och de fördelar som användare upplever genom att dela sin information (Cho et al., 2018).

Genom att använda en forskningsmetod som är influerad av kvantitativa metoder kan vår studie samla in data från en stor användargrupp av träningsapplikationer för att undersöka dess påverkan på användarupplevelse och förtroende. Denna metod möjliggör inte bara att kunna generalisera resultaten över en större population, vilket är avgörande för att dra bredare slutsatser från studien, utan den tillåter även datainsamling från ett stort antal deltagare på kort tid (Lakshman et al., 2000). Enligt Oates (2006) erbjuder en kvantitativ dataanalys vetenskaplig trovärdighet och bygger på väl etablerade tekniker. Signifikanstester ger förtroende för resultaten, vilket bygger på mätbara kvantiteter, inte subjektiva intryck, och

statistiska tester kan granskas av andra. Eftersom kvantitativa metoder fokuserar på mätbara data är det dock svårt att få utrymme för de underliggande orsakerna och sammanhangen bakom svaren. Detta till skillnad mot kvalitativa metoder där respondenterna får möjlighet till öppna svar under vägledning av en intervjuare, vilket tillåter en mer detaljerad insikt i svaren (Jacobsen, 2002).

Enligt Jacobsen (2002), är kvantitativa metoder begränsade i sin förmåga att erhålla djupare insikter i användarnas svar. Syftet med denna studie är inte att analysera de underliggande orsakerna till användarnas svar, utan att få en övergripande förståelse för hur datainsamling inom träningsapplikationer påverkar användarnas intention att dela data. Därmed kan den kvantitativa forskningen ge en mer omfattande och objektiv förståelse för de utforskade aspekterna.

3.3 Population och urval

Studien har som syfte att undersöka användare av träningsapplikationer i Sverige. Om målet hade varit en internationell undersökning hade populationen uppgått till cirka 330 miljoner användare (Curry, 2024). Eftersom det hade skapat stora utmaningar att stratifiera ett urval som är representativt för den internationella populationen, avgränsade vi oss till populationen av svenska användare. Eftersom studien undersöker även sällananvändare är data om dagliga användare inte av intresse utan snarare användare sett över ett kalenderår. Då uppgår populationen till ca 2.9 miljoner användare (Statista, 2024).

I genomsnitt använder 33 % av befolkningen i alla åldersgrupper träningsapplikationer. Bland de största åldersgrupperna, de mellan 20 till 29 och 30 till 39 år, använder 39 respektive 42 % träningsapplikationer. Användningen inom de övriga åldersgrupperna varierar mellan 21 % och 28 % (Fung Global Retail & Technology, 2017). Omräknat till vår populationsfördelning skulle det se ut så här:

- <18 år 14,7 %
- 18–24 år 14,6 %
- 25–34 år 22 %
- 35–44 år 22,9 %
- 45–54 år 14,8 %
- 55–64 år 12,9 %
- 65 + år 5,9 %

Dessa procentandelar har erhållits från en internationell studie, men vi bedömer att de tillhandahåller en relevant representation även för den svenska delen av populationen som vår studie fokuserar på. De källor som visar könsfördelningen inom träningsapplikationer gör det inte på ett globalt plan utan mäter specifika länder. För att få en rimlig representation utgår vi från könsfördelningen inom Sveriges befolkning där fördelningen är 49,65 % kvinnor och 50,35 % män (Statistiska Centralbyrån, 2023).

Med hänsyn till tidsramen valde vi att genomföra ett bekvämlighetsurval. Detta tillvägagångsätt visade sig vara det mest praktiska, och för att distribuera enkäten använde vi oss av träningsrelaterade grupper på Facebook. Detta möjliggjorde att vi kunde nå individer som använder träningsapplikationer.

3.4 Enkätutformning

För att kunna få svar på individers attityder till risker och fördelar kopplat till Privacy Calculus Theory behövde vi forma enkäten utifrån de olika delar som ingår i teorin. Eftersom frågeställningen inte specificerar hur ofta användaren behöver använda träningsapplikationer utformades svaren utifrån att användaren åtminstone använder träningsapplikationer en gång om året. På så vis kunde vi undersöka den breda massan och inte bara aktiva användare. Det var viktigt då vi kunde mäta om det fanns ett samband mellan exempelvis träningsfrekvens och intentionen att dela information. För att kunna undersöka eventuella samband mellan ålder och attityder till träningsapplikationer har vi valt svarsalternativ i olika åldersspann. För att kunna se om det finns eventuella samband mellan kön och attityder och har därför med en fråga om kön, där det finns tre alternativ: Man, kvinna eller ”vill ej uppge”.

Med utgångspunkt i tidigare forskning (Cho, 2018) har frågeformuläret (se tabell 3.1) utformats för att mäta fem olika områden, upplevt värde, oro för integritet, avsikt att dela information, upplevd användbarhet, och datadelning med tredje part. Detta för att kunna göra sambandsanalyser utifrån teorins ramverk.

Tabell 3.1: Enkätutformning (anpassad utifrån Cho et al., 2018)

Konstrukt	Frågor	Förklaring
Perceived Value	PV1	Jämfört med riskerna med att min information avslöjas är användningen av träningsappar fördelaktig för mig.
	PV2	Jämfört med den information jag behöver avslöja erbjuder användningen av träningsappar värde för mig.
	PV3	Sammantaget levererar användningen av träningsappar ett bra värde för mig.
Privacy Concern	PC1	Jag är orolig att min information som samlats in av träningsappar kan missbrukas.
	PC2	Jag är orolig över att tillhandahålla min information till träningsappar eftersom den kan användas på ett sätt jag inte förutsåg.
	PC3	Jag är orolig över att lämna information till träningsappar på grund av vad andra kan göra med den.
Intention to Disclose Information	ID1	Jag är benägen att avslöja min information genom att använda träningsappar.
	ID2	Jag är intresserad av att avslöja min information till träningsappar.
	ID3	Jag avser att fortsätta tillhandahålla min information.
	ID4	Jag är villig att avslöja min information för att fortsätta använda träningsappar.
Perceived Usefulness	PU1	Träningsappar är mycket användbara för min träning.
	PU2	Träningsappar tillhandahåller mycket användbar service och information till mig.
	PU3	Att använda träningsappar förbättrar kvaliteten på träningen.
Secondary Use of Information	SU1	Jag är orolig att träningsappar kan använda min information för andra ändamål utan att meddela mig eller be om min tillåtelse.
	SU2	När jag ger min information till träningsappar är jag orolig att den kan använda min information för andra ändamål.
	SU3	Jag är orolig att träningsappar kan dela min information med andra utan att erhålla min tillåtelse.

3.5 Datainsamling och analys

För att kunna besvara uppsatsens forskningsfråga behöver litteraturen och teorier som används kompletteras med empiriska data från användare av träningsapplikationer. För att kunna applicera Privacy Calculus Theory på vår forskningsfråga behöver vi statistik från aktiva användare om hur de ser på fördelar, risker, intentioner och användbarhet. För att kunna få en bild över huruvida ålder och kön påverkar dessa faktorer kommer detta vara med i datainsamlingen. Vi vill skapa en allmän bild över hur användares upplevelse och förtroende påverkas av träningsapplikationers datainsamling. Vi vill även skapa en bild över vilka funktioner som används och om det finns skillnader i upplevda fördelar och risker beroende på vilka funktioner man använder.

Efter att ha samlat in svaren från vår enkät, har dessa kodats om i Google Spreadsheet för att beräkna ett medelvärde som visar på den generella positiva eller negativa uppfattningen bland användarna av träningsapplikationer. Därefter omkodade vi svaren från 'instämmer i hög grad', 'håller delvis med', 'neutral', 'instämmer delvis', och 'instämmer inte alls' till en skala från 1 till 5, där 'neutral' har värdet 3. Denna omkodning har gjort det möjligt för oss att skapa en genomsnittlig värdering av användarnas uppfattning om följande områden: upplevt värde, oro för integritet, avsikt att dela information, upplevd användbarhet och oro för datadelning med tredje part. För analys och presentation av data har verktyget Google Spreadsheet använts.

3.5.1 Svarsfrekvens och bortfall

För att maximera vår svarsfrekvens och undvika bortfall av respondenter valde vi att skapa en tydlig struktur och undvika fritext-svar för att dels kunna styra strukturen men också för att spara tid för respondenten. För att tydliggöra enkätens syfte valde vi att ha en introduktion där vi förklarar vad vi undersöker och vad svaren kommer att användas till. Vi klargjorde på förhand hur lång tid det skulle ta för respondenten att svara. Detta för att skapa rätt förväntningar och undvika att respondenter ger upp på förhand eller under tidens gång. Vi hade 20 frågor där två handlade om ålder och kön.

Vi skickade ut enkäten i olika träningsgrupper på sociala medier för att kunna nå ut till träningsintresserade individer. Detta gjorde också att vi enkelt kunde undvika de som inte använder träningsapplikationer. Dock påverkade detta genom att vi inte kunde mäta bortfall och svarsfrekvens då vi inte har information om hur många enkäten nådde ut till.

3.5.2 Validitet och reliabilitet

Validitet avser graden av noggrannhet med vilken en enkät avspeglar det forskningsområde som avses att studeras. Det är avgörande att enkäten täcker alla aspekter av de ställda forskningsfrågorna och att varje enskild fråga mäter exakt det den är avsedd att mäta (Oates et al., 2006). För att säkerställa detta har vi granskat tidigare studier för att förstå hur andra forskare har närmat sig undersökningar med Privacy Calculus Theory kopplat till träningsapplikationer med forskningsfrågor som är relaterade till vår och baserat våra frågor på relevant litteratur. För att säkerställa reliabiliteten gjorde vi en statistisk reliabilitetsanalys (se figur 3.1). Resultatet visade ett Cronbachs Alpha på .852 som innebär att reliabiliteten är god, över 0.7 är acceptabelt och 9 är utmärkt (Christmann & Aelst, 2006). Cronbachs Alpha

baserat på standardiserade punkter gav .855 vilket bekräftar konsekvent tillförlitlighet oavsett om punkterna är standardiserade eller inte.

Case Processing Summary

		N	%
Cases	Valid	206	100.0
	Excluded[a]	0	.0
	Total	206	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.852	.855	16

Figur 3.1: Reliabilitetsanalys

3.6 Etiska överväganden

Vi har beaktat de etiska aspekterna i vår metod för att säkerställa att respondenterna känner sig trygga, för att upprätthålla lagliga krav och för att minimera risken för bortfall i svarsfrekvensen. Enligt Oates et. al (2006) finns det fem grundläggande rättigheter för respondenter: rätten att avstå från deltagande, rätten att när som helst avbryta sitt deltagande, rätten att ge informerat samtycke, rätten till anonymitet och rätten till konfidentialitet.

I vår undersökning var rätten att inte delta självklar; deltagande kräver att respondenterna aktivt öppnar, besvarar och sänder in sina svar på enkäten. Vi tvingade inte någon att starta eller slutföra enkäten; deltagarna kunde avsluta den när som helst, vilket automatiskt eliminerade alla deras tidigare svar. Informerat samtycke erhölls när respondenterna skickade in sina svar, vilket vi klargjorde i enkätens introduktion. Vi garanterade anonymitet genom att inte samla in några personliga uppgifter bortsett från ålder och kön.

I enlighet med GDPR kommer vi inte lagra några personuppgifter och svaren kommer endast framställas i tabeller och grafer.

3.7 Publicering av enkät

För att nå ut med vår enkätundersökning valde vi att publicera den i flera specifika Facebookgrupper, vilka var noga utvalda baserat på deras relevans för undersökningens tematik kring träning och hälsa. Totalt publicerades enkäten i följande grupper (se tabell 3.2):

Tabell 3.2: Facebookgrupper 1

Grupp	Antal medlemmar
TräningsGlädje & Inspiration	69 300
Tränande Veganer	10 800
Team Snigel	2 900
Träning, motivation & inspiration	7 900
Livslång träning och hälsa	7 800
Motivation och träning och kost	11 100
Träning Hälsa & Kost	37 500
Totala antalet medlemmar	= 147 300

Enkäten publicerades i samtliga ovan nämnda grupper den 9 april med en räckvidd på 147 300 individer. För att maximera synligheten och säkerställa det önskade antalet respondenter, avlägsnades det ursprungliga inlägget efter en vecka och enkäten publicerades om i samtliga grupper. Enkäten avslutades den 23 april 2024, och vid tidpunkten för analysen hade totalt 209 svar samlats in från respondenterna.

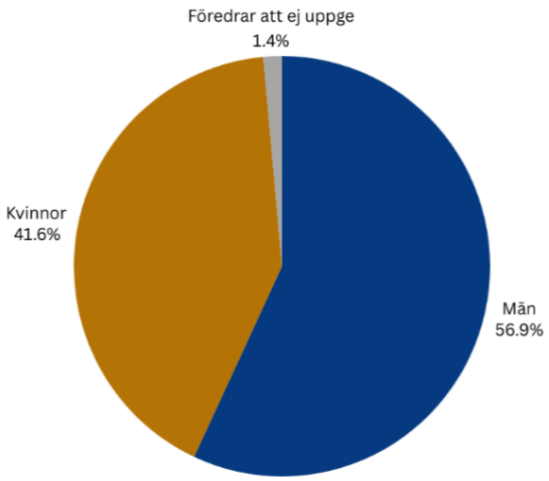
4 Empiri

I följande del presenteras resultaten från den kvantitativa undersökningen. Vi hade som mål att samla in svar från minst 150 deltagare. Denna målsättning överträffades, och totalt erhölls 209 svar från respondenterna. Vi har använt oss av Likertskalan för att samla in data i vår undersökning. Likertskalan, som diskuteras av Sullivan et. al (2013), är en vanlig förekommande mätmetod för att samla in data om individers åsikter och attityder. Denna metod innefattar flera svarsalternativ, vilka varierar från 'instämmer i hög grad' till 'instämmer inte alls'. Skalan är en 5-punktsskala där varje grad representerar en ökande nivå av enighet.

I vår undersökning har vi valt att fokusera på områden som är relevanta för användarens interaktion med träningsapplikationer. Dessa inkluderar användarnas upplevda värde av applikationen, oro för personlig integritet, avsikt att dela information, upplevd användbarhet samt datadelning med tredje part. Valet av dessa specifika delar i vår undersökning grundar sig i den teoretiska referensramen Privacy Calculus Theory (Cho et al., 2018), för att förstå hur individer väger upplevda fördelar mot risker i samband med att avslöja personlig information. Denna referensram är särskilt relevant i kontexten av olika digitala träningstillbehör såsom träningsapplikationer och smartklockor, där användarnas beslut att dela data är kritiskt (Cho et al., 2018).

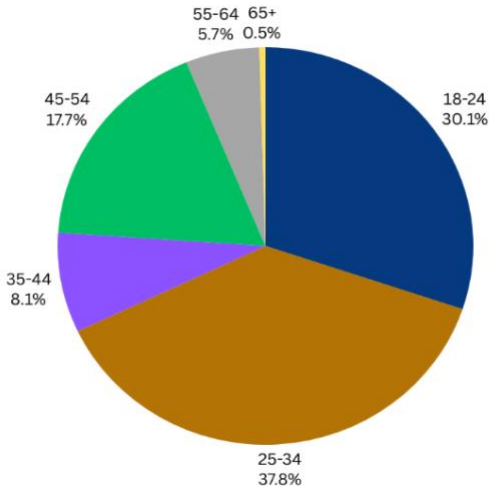
4.1 Ålder och kön

Av de totalt 209 respondenterna identifierade sig 119 som män och 87 som kvinnor, medan de återstående tre respondenterna valde att inte specificera sitt kön (se figur 4.1).



Figur 4.1: Könsidentitet hos respondenter

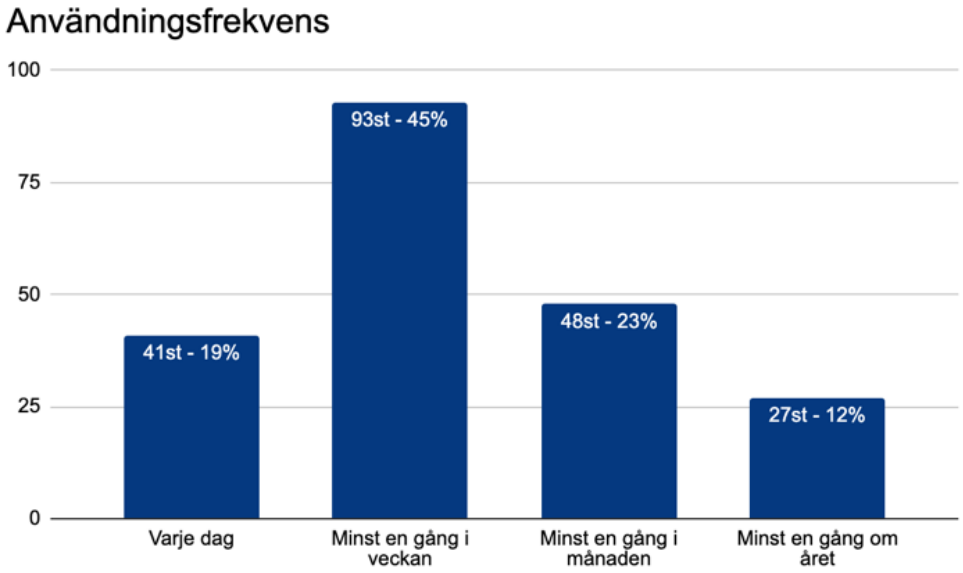
Bland deltagarna fanns 63 individer i åldersgruppen 18 till 24 år, 79 individer i åldersgruppen 25 till 34 år, 17 individer i åldersgruppen 35 till 44 år, 37 individer i åldersgruppen 45 till 54 år och 12 individer i åldersgruppen 55 till 64 år. Endast en respondent var 65 år eller äldre och inga respondenter var under 18 år (se figur 4.2).



Figur 4.2: Ålder hos respondenterna 1

4.2 Användning och funktioner

Av våra respondenter använder 134 individer träningsapplikationer varje dag eller minst en gång i veckan vilket tyder på att de som svarat på enkäten är regelbundna användare av dessa applikationer. Vi har utöver det fått in 48 individer som använder träningsapplikationer en gång i månaden och 27 individer som använder träningsapplikationer minst en gång per år (se figur 4.3).



Figur 4.3: Användning av träningsapplikationer

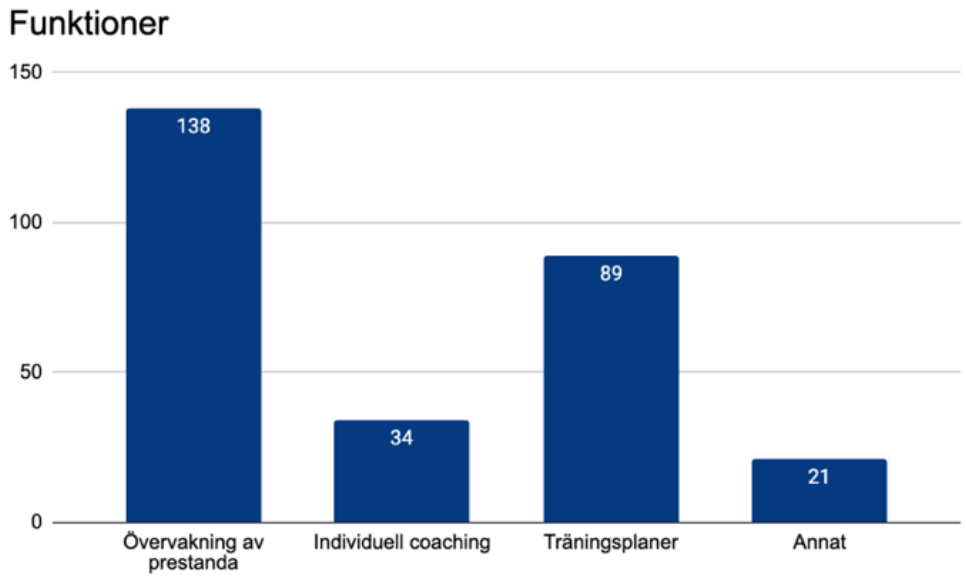
Av de funktioner som finns i en träningsapplikation har vi valt att använda oss av övervakning av prestanda, individuell coaching och träningsplaner som alternativ i vår undersökning (se figur 4.4). Respondenten har i denna fråga möjlighet att välja en eller flera funktioner.

Övervakning av prestanda - Innebär att applikationen samlar in och analyserar data om användarens fysiska aktiviteter, såsom löptid, antal steg, kaloriförbränning och hjärtfrekvens.

Individuell coaching - Innebär att applikationen erbjuder personlig träning och vägledning. Detta kan vara genom förinspelade videor eller genom realtidssessioner med en tränare via applikationen.

Träningsplaner - Förutbestämda eller anpassningsbara program som är utformade för att hjälpa användare att uppnå specifika träningsmål, som att förbättra kondition, bygga muskelstyrka, eller gå ner i vikt.

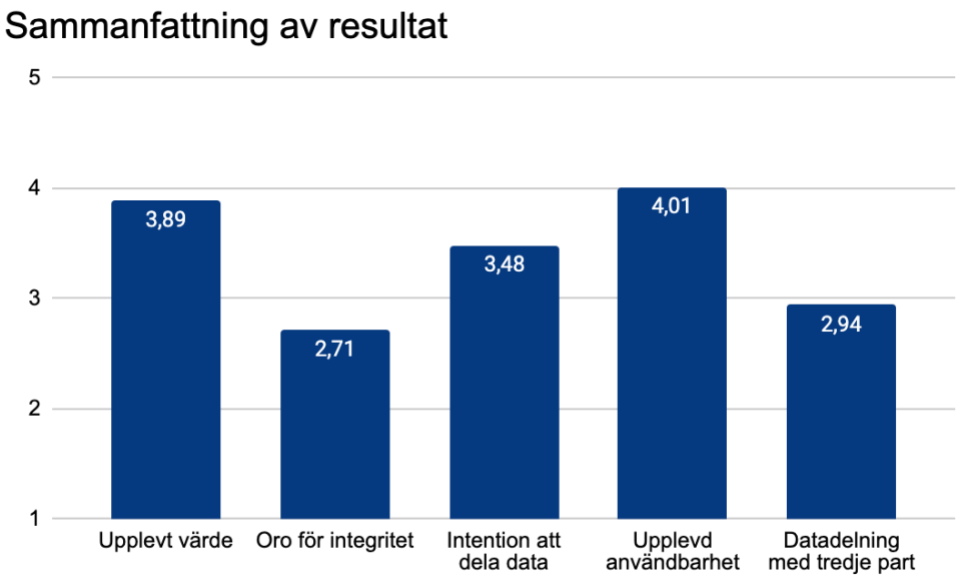
I undersökningen angav 138 respondenter att de använde funktionen för övervakning av prestanda, 34 respondenter valde individuell coaching, 89 respondenter använde sig av träningsplaner, och 21 respondenter valde andra funktioner som inte listats ovan.



Figur 4.4: Funktioner 1

4.3 Sammanfattning av resultat

Figur 4.5 presenterar ett medelvärde av respondenternas uppfattningar om träningsapplikationer, inklusive det genomsnittliga värdet för upplevt värde, där respondenterna har utvärderat de fördelar de upplever i jämförelse med den information de behöver avslöja. Figuren inkluderar även genomsnittsvärden för respondenternas oro för personlig integritet, deras avsikt att dela personlig information, upplevda användbarhet av träningsapplikationer samt oro kring sekundär användning av deras personliga information.



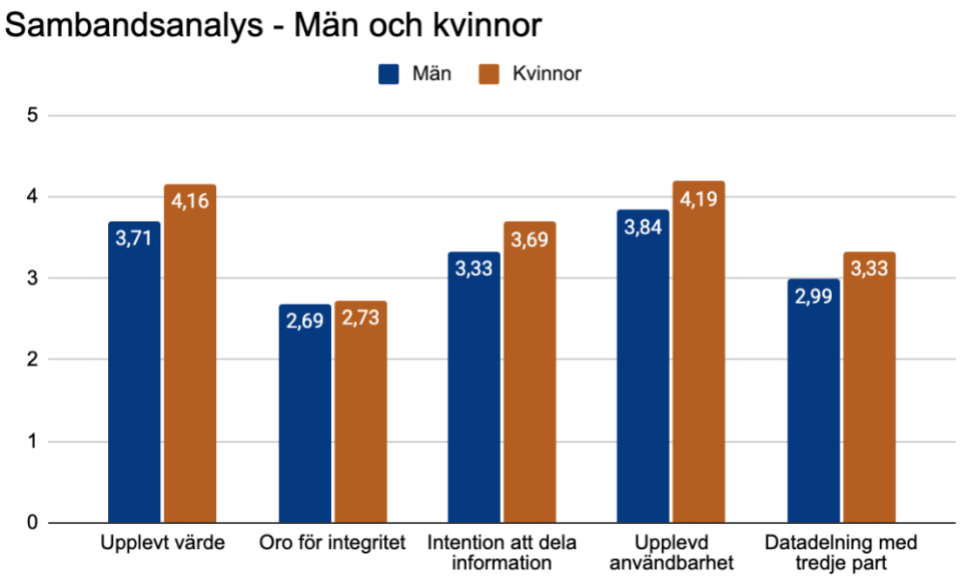
Figur 4.5: Medelvärdet av respondenternas sammanfattade uppfattning

4.4 Sambandsanalys

I vår sambandsanalys kommer vi att undersöka hur bakgrundsvariablerna ålder, kön och användningsfrekvens påverkar riskbedömningen hos användarna av träningsapplikationer. En sambandsanalys enligt (Pandey, 2020) används och är bra för att mäta relationen mellan olika variabler och deras mönster. Denna sambandsanalys baseras på Privacy Calculus Theory, som antyder att individer gör en avvägning mellan den upplevda nyttan och riskerna när de beslutar sig för att dela personlig information (Cho et., al 2018). De fem olika områden som vi mäter är upplevt värde, oro för integritet, avsikt att dela information, upplevd användbarhet, och datadelning med tredje part.

4.4.1 Kön

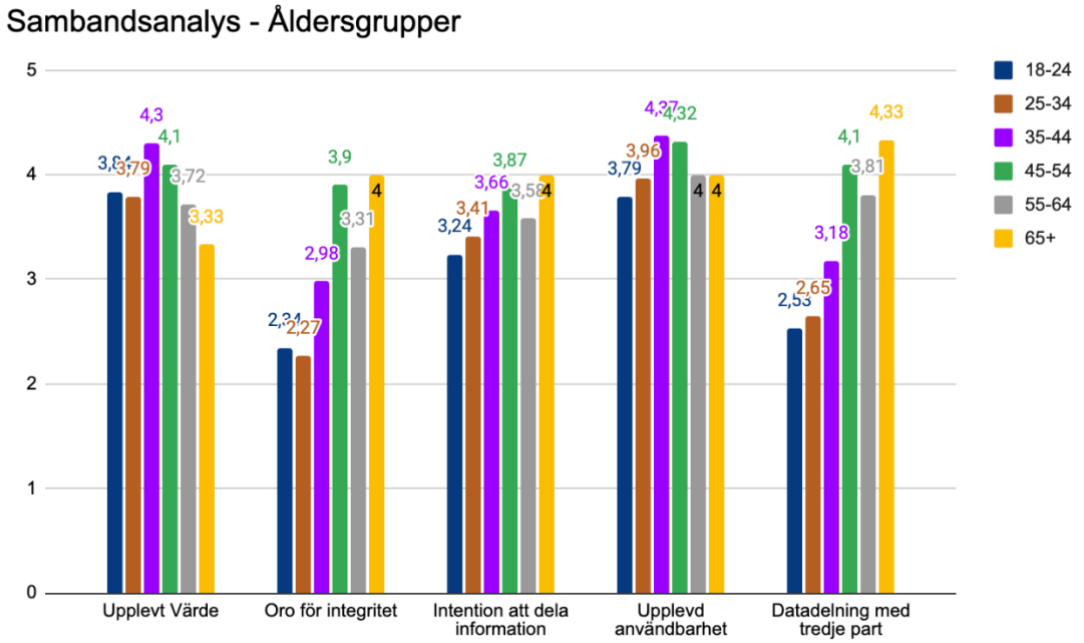
Figur 4.6 presenterar ett medelvärde mellan män och kvinnors uppfattningar om träningsapplikationer. Denna figur inkluderar de genomsnittliga värdena för uppfattat värde av träningsapplikationer, användarnas oro för personlig integritet, benägenheten att avslöja personlig information, upplevd användbarhet av applikationerna, samt oro för sekundär användning av insamlad information.



Figur 4.6: Sambandsanalys - Könsidentitet

4.4.2 Ålder

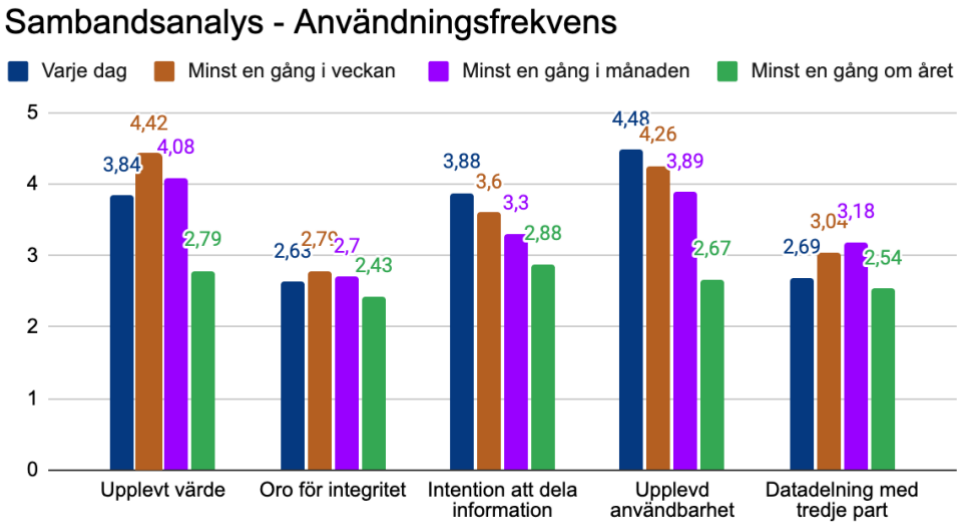
Figur 4.7 presenterar ett medelvärde över olika åldersgruppers uppfattningar om träningsapplikationer. Figuren inkluderar de genomsnittliga värdena för uppfattat värde av träningsapplikationer, användarnas oro för personlig integritet, benägenheten att avslöja personlig information, upplevd användbarhet av applikationerna, samt oro för sekundär användning av insamlad information.



Figur 4.7: Sambandsanalys- Åldersgrupper 1

4.4.3 Användningsfrekvens

Figur 4.8 presenterar ett medelvärde av användarnas åsikter i relation till träningsapplikationer, grupperat efter användningsfrekvens. Figuren inkluderar de genomsnittliga värdena för uppfattat värde av träningsapplikationer, graden av oro för integritet, användarnas avsikt att dela personlig information, upplevd användbarhet av applikationerna, samt inställningen till datadelning med tredje part.



Figur 4.8: Sambandsanalys - Användning 1

4.5 Korrelationstabell

Tabell 4.1 visar en korrelationstabell, vilket är ett verktyg för att visualisera och analysera samband mellan olika variabler i en datamängd. Varje cell i matrisen representerar korrelationskoefficienten mellan två variabler. Korrelationskoefficienten, som kan variera mellan -1 och 1, indikerar styrkan samt riktningen på sambandet mellan variablerna. En positiv koefficient (närmare 1) visar på ett starkt positivt samband, medan en negativ koefficient (närmare -1) visar på ett starkt negativt samband. En koefficient nära 0 tyder på att det inte finns något samband.

Tabell 4.1: Korrelationstabell

	Mean	**PV**	**PC**	**ID**	**PU**	**SU**
PV	3,89					
PC	2,71	-0,07				
ID	3,48	0,59***	0,04			
PU	4,01	0,65***	0,07	0,51***		
SU	2,94	-0,12	0,83***	0,01	0,08	

***p<.001

Perceived Value och Intention to Disclose Information (0.59)

Det finns en måttligt positiv korrelation mellan hur värdefull informationen uppfattas vara och intentionen att avslöja informationen. Detta kan tyda på att ju mer värdefull informationen uppfattas, desto större är viljan att dela den.

Perceived Value och Perceived Usefulness (0.65)

Det finns även en stark positiv korrelation mellan uppfattat värde och uppfattad användbarhet. Detta är logiskt då information som uppfattas som värdefull också ofta ses som användbar.

Privacy Concern och Secondary Use of Information (0.83)

En mycket stark positiv korrelation här indikerar att oro för sekretess är starkt kopplad till sekundär användning av information. Det betyder att högre oro för hur informationen kan användas sekundärt ökar när oron för sekretess ökar.

Intention to Disclose Information och Perceived Usefulness (0.51)

Det finns en positiv korrelation som visar att ju mer användbar träningsapplikationen uppfattas vara, desto större är benägenheten att dela med sig av den. Detta stödjer idén att användbar information är mer benägen att delas.

Perceived Value och Secondary Use of Information (-0.12)

En svagt negativ korrelation här kan tyda på att när informationen uppfattas som värdefull, finns det en liten tendens att oroa sig för informationens sekundära användning. Detta kan vara beroende av kontext eller typ av information.

Privacy Concern Mean och Perceived Value Mean (-0.07)

Här finns nästan ingen korrelation, vilket tyder på att dessa två faktorer är relativt oberoende av varandra.

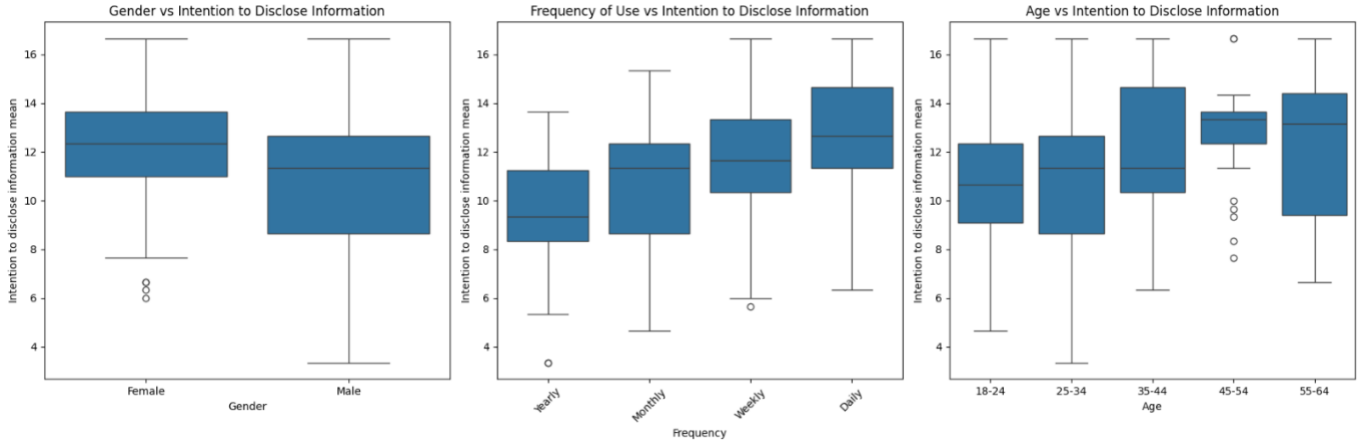
Figur 4.9 består av tre låddiagram som visar sambandet mellan olika demografiska och beteendemässiga faktorer och intentionen att dela information. Varje diagram representerar en specifik variabel:

Kön och intention att dela information: Det första diagrammet jämför intentionen att dela information mellan kvinnliga och manliga deltagare. Medianvärdena samt spridningen och utliggarna (extrema värden) visas, vilket indikerar variationer i avsikterna mellan könen.

Användningsfrekvens och. intention att dela information: Det andra diagrammet utforskar sambandet mellan hur ofta individer använder en tjänst eller produkt (sällan, veckovis, dagligen) och deras intention att dela information. Detta diagram ger insikt om hur användningsfrekvensen kan påverka intentionerna att dela information.

Ålder och. intention att dela information: Det tredje diagrammet delar in deltagarna i åldersgrupper och visar deras intention att dela information. Detta kan ge en uppfattning om hur olika åldersgrupper förhåller sig till informationsdelning.

Varje box i diagrammen representerar kvartilvärdena för datadistributionen, där lådan sträcker sig från första till tredje kvartilen och medelstrecket indikerar medianen. Utliggarna (markerade med cirklar) representerar data som ligger utanför den vanliga spridningen och kan indikera exceptionella fall. Genom dessa diagram kan forskare och analytiker dra slutsatser om hur olika faktorer påverkar avsikten att avslöja personlig information i olika grupper



Figur 4.9: Regression låddiagram

Kön

Kvinnor: Figur 4.9 visar en högre median och ett bredare intervall, vilket tyder på att kvinnor generellt har en högre avsikt att avslöja information jämfört med män. Förekomsten av outliers under lådan tyder på att det finns vissa kvinnor med särskilt låga avsiktsnivåer, som skiljer sig avsevärt från majoriteten.

Män: Medianavsikten att avslöja information bland män är lägre än för kvinnor. Intervallet är smalare, vilket tyder på mindre variabilitet bland män jämfört med kvinnor.

Frekvens

Årligen: Användare som deltar årligen visar ett brett spektrum av avsikter, med en median som tyder på en måttlig avsiktsnivå att avslöja information.

Månadsvis: Liknande årliga användare, men med en något högre median, vilket indikerar en något starkare avsikt att avslöja information.

Veckovis: Denna grupp visar en lägre medianavsikt jämfört med månatliga användare, vilket kan vara oväntat eftersom mer frekvent användning kan innebära högre engagemang och möjligen en högre avsikt att avslöja.

Dagligen: Användare som använder tjänsten dagligen uppvisar en högre medianavsikt, vilket överensstämmer med förväntningarna att mer frekvent användning korrelerar med högre engagemang och vilja att avslöja information.

Ålder

18-24: Yngre användare visar en betydande spridning i avsikt, med en relativt lägre median, vilket tyder på varierande nivåer av komfort eller vilja att avslöja information.
25-34: Denna åldersgrupp har en högre medianavsikt än 18-24-gruppen, vilket indikerar en större vilja att avslöja information.

35-44: Liknande 25-34-gruppen men med en något lägre median. Spridningen är också mindre, vilket tyder på mer konsekvens i deras svar.

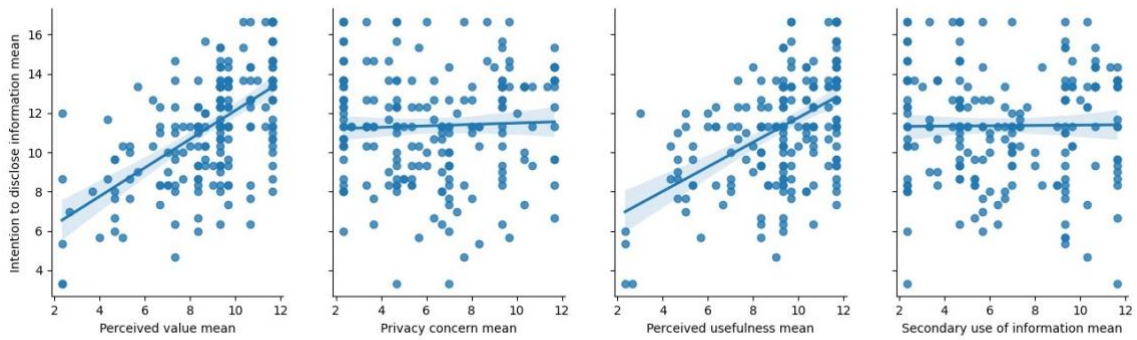
45-54: Denna grupp har den högsta medianavsikten att avslöja information. Det finns dock märkbara utliggare i både de höga och låga ändarna, vilket tyder på viss variabilitet inom gruppen.

55-64: Äldre användare visar generellt höga avsikter liknande 45-54-gruppen men med mindre variabilitet, som ses i det mindre interkvartilintervallet.

Det finns en trend där avsikten att avslöja information tenderar att öka med åldern, med viss variation. Kön och användningsfrekvens spelar också viktiga roller i avsikten att avslöja information. Män visar generellt en lägre avsikt över alla frekvenser jämfört med kvinnor. Utliggare i data tyder på att det finns undantagsfall i varje grupp som avviker avsevärt från de allmänna trenderna, vilket skulle kunna motivera ytterligare undersökningar för att förstå deras orsaker eller implikationer.

4.6 Regressionsanalys

Figur 4.10 består av fyra spridningsdiagram som visar sambandet mellan användares intention att dela information med (vertikal axel) och fyra olika variabler (horisontell axel): upplevt värde, integritetsoro, upplevd användbarhet och sekundär användning av information. Diagrammen illustrerar hur dessa faktorer potentiellt kan påverka användarens intention att dela information. Varje diagram inkluderar en trendlinje som ger en visuell indikation på det generella sambandet mellan variablerna. Till exempel antyder en positiv lutning på trendlinjen en ökad benägenhet att dela information eftersom det upplevda värdet eller användbarheten av informationen ökar.



Figur 4.10: Regressionsanalys

Koefficienter och deras P-värden:

Konstant (const)

Koefficient: 3,6129

P-värde: <0,000

Detta mycket låga P-värde indikerar att konstanten är statistiskt signifikant. När alla oberoende variabler är noll, är den genomsnittliga förväntade nivån på "Intention to disclose information mean" cirka 3,613.

Perceived Value

Koefficient: 0,5718

P-värde: <0,000

Denna variabel är mycket signifikant och har en stark positiv effekt på intentionen att avslöja information. Det visar att ökande värdeuppfattning starkt ökar benägenheten att dela data.

Privacy Concern

Koefficient: 0,0510

P-värde: 0,585

P-värdet tyder på att integritetsoro inte har en statistiskt signifikant påverkan på intentionen att dela information. Detta kan innebära att användare kanske väger andra faktorer högre än sina privatlivsbekymmer när de bestämmer sig för att dela information.

Perceived Usefulness

Koefficient: 0.2453

P-värde: 0.008

Den upplevda användbarheten har en signifikant positiv effekt på intentionen att dela information. Detta indikerar att när användare upplever en applikation eller tjänst som användbar, är de mer benägna att dela sin information.

Secondary Use of Information

Koefficient: 0.0019

P-värde: 0.984

Denna variabel är inte statistiskt signifikant, vilket tyder på att sekundär användning av information inte påverkar användares intention att dela sin information. Detta kan peka på att användare kanske inte är medvetna om eller inte oroar sig för hur deras information kan användas i andra sammanhang.

5 Diskussion

5.1 Metoddiskussion

Vår studie är influerad av en kvantitativ forskningsdesign för att utforska hur upplevd risk och upplevt värde påverkar användares intention att dela data med träningsapplikationer. Ett centralt teoretiskt ramverk i vår studie är Privacy Calculus Theory, vilket hjälper oss att förstå hur användare väger fördelarna med användning mot de potentiella integritetsriskerna (Cho et al., 2018). Denna teori är särskilt relevant i vår kontext eftersom träningsapplikationer kontinuerligt hanterar känslig personlig information.

En viktig aspekt av vår metodik är användningen av enkätundersökningar för att samla in data, vilket stöds av Lakshman (2002), som betonar kvantitativa metoders förmåga att generera generaliserbara och objektiva data över stora populationer. Dock, som med alla forskningsmetoder, finns det begränsningar i vårt tillvägagångssätt som kan påverka tolkningen av resultaten. Slutligen kan vår studie ha begränsningar i att djupare utforska de underliggande orsakerna och sammanhangen bakom användarnas svar, något som mer utförligt kan hanteras genom kvalitativa forskningsmetoder (Jacobsen, 2002).

Privacy Calculus Theory, som är central i vår analys, hjälper oss att diskutera hur individer gör avvägningar mellan personlig integritet och upplevda fördelar. Enligt denna teori, om de upplevda fördelarna anses större än de upplevda riskerna, är användare mer benägna att fortsätta att dela sin information (Cho et al., 2018). Detta reflekteras i våra resultat där användare visar en vilja att acceptera vissa integritetsrisker. Vår studie bidrar till den existerande litteraturen genom att tillämpa Privacy Calculus Theory inom en ny kontext av träningsapplikationer och genom att utforska den generella uppfattningen samt hur de olika demografiska grupperna upplever denna avvägning.

5.2 Sammanfattning av resultatet

I vår studie har vi identifierat att användare generellt uppfattar ett positivt värde av att använda träningsapplikationer, vilket visas av genomsnittsvärdet 3,89 för upplevt värde i Figur 4.5. Denna positiva inställning är i linje med Yang et al. (2016), som framhåller hur upplevd nytta och funktionalitet kan främja en positiv användarupplevelse och öka acceptansen för teknologi trots potentialen för datadelning. Resultaten stärker ytterligare denna observation och stöds av Zimmer et al. (2018) som fann att fördelarna med träningsklockor och applikationer ofta upplevs som större än nackdelarna.

Samtidigt framkommer en ökad oro för integritetsrisker, som avbildas i figur 4.5 med ett värde på 2,71 under oro för integritet. Denna oro speglar in med Schomakers et al. (2021), som undersöker hur integritetsoro påverkar användares acceptans för smarta teknologier. Användare gör en avvägning mellan personliga fördelar, såsom övervakning av personlig hälsa och risker relaterade till personlig integritet. Stach (2018) betonar hur träningsapplikationer ofta hanterar känslig information utan tillräckliga skyddsåtgärder. Trots detta visar figur 4.5 att majoriteten, med ett genomsnitt på 3,48 under 'intention att dela information', fortfarande är villiga att dela med sig av sin information, vilket speglar en avvägning där de upplevda fördelarna anses överväga de potentiella riskerna. Stach (2018) stöder vår undersökning och tar upp vikten av att implementera Privacy Policy Models och Privacy Management Platform som kan skydda användardata. Mitschang och Stach (2014) diskuterar också vikten av att utforma dessa plattformar på ett transparent och användarcentrerat sätt för att öka användarnas förtroende och acceptans. Detta bygger vidare på Abdelhamid (2021), som visar att när användare känner att de har detaljerad kontroll över sina data, ökar också fortsatt användning.

Sammanfattningsvis kompletterar och förstärker denna studie tidigare forskning genom att illustrera dynamiken mellan användarnas upplevda fördelar och risker vid användning av träningsapplikationer.

5.3 Kön

Enligt resultaten från Figur 4.8, uppfattar kvinnor fördelarna och användbarheten av träningsapplikationer högre än män, med genomsnittsvärden på 4,16 för fördelar och 4,19 för användbarhet, jämfört med mäns 3,71 och 3,84 i samma kategorier. Denna skillnad i uppfattning stöds av Harris et al. (2006), som visar att kvinnor generellt är mer benägna att engagera sig i aktiviteter med positiva utfall och tenderar att värdera dessa fördelar högre. Denna större uppskattning av teknikens potential att förbättra hälsa och välbefinnande hos kvinnor kan också spegla en mer optimistisk syn på hur tekniken kan användas för personlig utveckling.

Undersökningen visar även att kvinnor generellt uttrycker en högre nivå av oro för integritet, med ett genomsnitt på 2,73 för generell integritetsoro och 3,33 för oro över sekundär användning av information. Män visar något lägre nivåer av oro med genomsnitt på 2,69 och 2,99 i samma kategorier. Eckel och Grossman (2008) bekräftar att kvinnor tenderar att vara bättre på att identifiera och reagera på potentiella risker, vilket kan förklara deras högre grad av oro för integritetsfrågor.

Vidare visar undersökningen att kvinnor är mer villiga att dela sin information än män, med ett genomsnitt på 3,69 jämfört med mäns 3,33. Denna högre benägenhet hos kvinnor att dela personlig information kan ses som ett resultat av deras uppfattning att personliga fördelar överväger riskerna, vilket Harris et al. (2006) tidigare påpekat.

Resultaten från denna studie bekräftar tidigare forskning genom att visa att kön spelar en signifikant roll i hur individer uppfattar och hanterar risker associerade med digital teknologi. Kvinnors högre oro för integritet och samtidigt större uppskattning av fördelarna med träningsapplikationer tyder på att de har en mer komplex syn på avvägningen mellan nytta och risk. Studier av Harris et al. (2006) och Eckel och Grossman (2008) ger viktiga insikter

om att kvinnor inte bara är mer riskmedvetna, utan även tenderar att aktivt söka och uppskatta teknik som förbättrar deras livskvalitet.

5.4 Ålder

Denna del av studien belyser hur olika åldersgrupper uppfattar och hanterar användningen av träningsapplikationer, med särskild fokus på deras uppfattningar av fördelar jämfört med potentiella risker. Figur 4.7 visar att medelålders användare (35–54 år) särskilt värderar de positiva aspekterna av träningsapplikationer, vilket speglas i deras höga genomsnittsvärden för upplevd användbarhet och uppskattning av applikationerna. Denna positiva inställning och dess korrelation med ålder bekräftas av Zeissig et al. (2017), som noterar att ålder spelar en avgörande roll i hur digital teknik värderas.

I kontrast till detta visar Figur 4.7 att äldre åldersgrupper (45–64 och 65+) uttrycker en högre grad av oro för integritetsintrång, medan yngre åldersgrupper (18–35) visar mindre oro. Denna tendens, som också bekräftar forskning av Boise et al. (2013), pekar på att äldre individer är mer försiktiga med att dela personlig information, vilket kan bero på en mer etablerad syn på privatliv och en starkare oro för integritet. Även åldersrelaterade skillnader i benägenheten att dela personlig information framkommer, där äldre användare visar större komfort med att dela, vilket kan spegla en mer mogen riskbedömning.

Slutligen påpekar undersökningen att äldre användare är mer bekymrade över sekundär användning av deras data utan medgivande, vilket visar på en högre medvetenhet och känslighet för integritetsfrågor bland denna grupp. Dessa resultat utmanar och berikar den befintliga litteraturen genom att detaljerat skildra hur ålder påverkar användarnas inställning till risker och fördelar med digital teknologi, vilket bekräftar tidigare observationer av både Boise et al. (2013) och Zeissig et al. (2017) om att äldre är mer försiktiga och att det finns åldersrelaterade skillnader i teknisk förtroende och riskuppfattning.

5.5 Användningsfrekvens

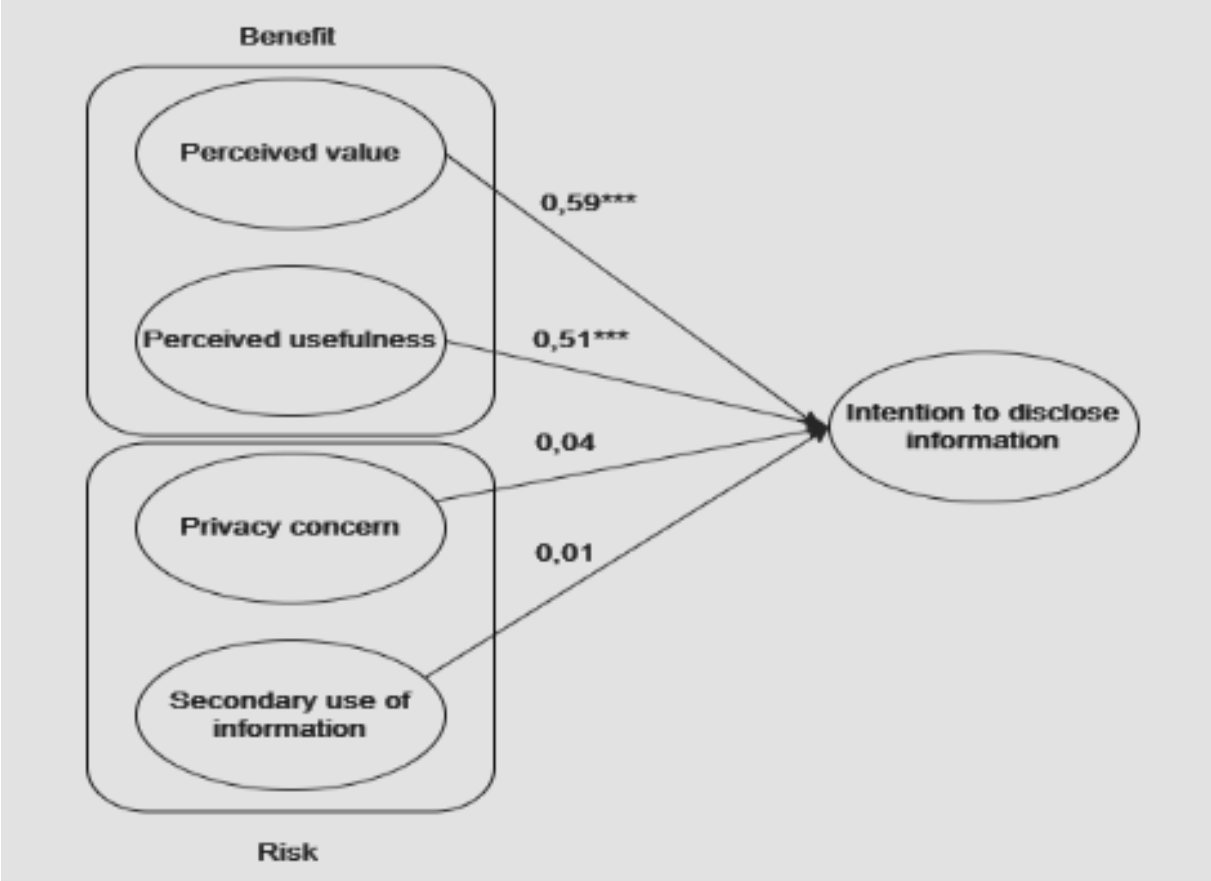
Resultaten från denna studie bekräftar och fördjupar förståelsen från Cho et al. (2018) om hur användningsfrekvens påverkar användarnas upplevelser och inställningar till träningsapplikationer. Figur 4.8 visar att personer som använder träningsapplikationer minst en gång i veckan eller månaden upplever ett högt värde i relation till riskerna och rapporterar en ökad användbarhet av tekniken, med genomsnittsvärden på över 4,0. Denna positiva upplevelse leder till att dessa användare tenderar att acceptera högre risker, vilket återspeglas i deras större benägenhet att dela information, noterat med ett genomsnitt på 3,88 för dagliga användare.

Å andra sidan visar undersökningen att de som använder applikationerna mindre frekvent, exempelvis minst en gång om året, uppvisar lägre oro för integritet och är mindre benägna att dela sin information, med genomsnittsvärden så låga som 2,43 respektive 2,88. Denna

information tydliggör hur olika användningsfrekvenser bidrar till varierande grad av oro för integritet och benägenhet att dela personlig information.

5.6 Regression

Resultaten av regressionsanalysen (se figur 5.1) visade att upplevt värde har en stark positiv effekt på användares intention att dela information. En ökad uppfattning av värde ökar benägenheten att dela data med stark effekt. Den visade också att upplevt värde är en mycket signifikant variabel. Vidare visade analysen att integritetsoro inte har en statistiskt signifikant påverkan på intentionen att dela information. Det kan innebära att användare kan väga andra faktorer högre än integritet när de bestämmer sig för att dela sin information. Upplevd användbarhet har en signifikant positiv effekt på intentionen att dela information, det indikerar att när en användare upplever en träningsapplikation som användbar, är de mer benägna att dela information. Variabeln sekundär användning av information är inte statistiskt signifikant vilket tyder på att den inte påverkar användarens intention att dela information. Detta kan innebära att användare inte är medvetna eller inte oroar sig för hur deras information kan användas i andra sammanhang än det aktuella.



Figur 5.1: Privacy Calculus Result

6 Slutsats och vidareforskning

6.1 Slutsats

Syftet med denna studie var att utforska hur upplevda risker och upplevda fördelar påverkar användares intentioner att dela data med träningsapplikationer. Vi undersökte även hur dessa avvägningar hanteras av olika användargrupper.

Resultaten från vår studie, tillsammans med tidigare forskning, visar att användarnas beslut att dela data drivs av en balans mellan de upplevda fördelarna och riskerna. Resultaten bekräftar att även om det finns en generell oro för integritetsrisker, är användarna beredda att dela personlig information om de upplever att fördelarna överväger riskerna. Denna avvägning är kärnan i Privacy Calculus Theory, vilket återspeglas i vårt resultat och understryker betydelsen av att användarnas uppfattningar om personlig nytta och risk kontinuerligt adresseras i design och utveckling av digitala lösningar.

Vår studie visar att regelbunden användning av träningsapplikationer korrelerar med en högre benägenhet att acceptera integritetsrisker, då frekventa användare upplever signifikanta fördelar. De som använder träningsapplikationer mer sporadiskt visar däremot lägre oro för integritet och är mindre benägna att dela information. Vidare framkom det att det finns skillnader i synen på datadelning baserat på kön och ålder. Kvinnor och äldre användare visar generellt högre oro för integritet och är mer försiktiga med att dela sin data jämfört med män och yngre användargrupper. Detta understryker hur demografiska faktorer kan påverka intentionen till att dela sin data.

6.2 Regression

Vår undersökning har begränsningar som bör beaktas när man tolkar resultaten. Urvalet var av deltagare begränsat till Sverige, vilket kan påverka generaliserbarheten av resultaten till andra kulturer eller geografiska regioner. Slutligen behandlar studien endast de intentioner som användare uttrycker, vilket inte nödvändigtvis motsvarar deras faktiska beteenden.

6.3 Förslag till vidareforskning

För att fördjupa insikterna inom datainsamling i träningsapplikationer skulle man kunna utföra kvalitativa intervjuer av användare. Även kvalitativa intervjuer med utvecklare för att addera det perspektivet. Samt ytterligare kvantitativ forskning knutet till ”continued use” som vi valde att inte ta med i forskningsmodellen.

Appendix 1 - Enkätundersökning

Undersökning av datainsamling hos träningsappar

Vi är två studenter som studerar sista terminen på Systemvetenskapliga kandidatprogrammet vid Lunds universitet. Vi skriver vårt examensarbete som undersöker datainsamling hos träningsappar. Svaren kommer att användas i vår undersökning om risker och fördelar i samband med användningen av träningsappar.

Vi hade blivit jätteglada om du hade kunnat svara på vår enkät. Enkäten är **anonym** och tar ca 5 minuter att svara på.

Stort tack på förhand!

English:

We are two student studying the last semester of the Bachelor's program in Systems Science at Lund University. We are currently writing our thesis which examines the data collection through fitness apps. The responses will be used in our survey on risks and benefits associated with the use of fitness apps.

We would greatly appreciate it if you would like to answer our survey. It's completely **anonymous** and takes about 5 minutes of your time.

Thanks in advance!

Kön/Gender *

- ○ Man/Male
- ○ Kvinna/Female
- ○ Föredrar att ej uppge/Prefer not to disclose

Hur gammal är du?
English:
How old are you?

- ◯ <18
- ◯ 18-24
- ◯ 25-34
- ◯ 35-44
- ◯ 45-54
- ◯ 55-64
- ◯ 65+

Vilka slags funktioner i träningsappar använder du? *
English:
What kind of features in fitness apps do you use?

- ☐ Övervakning av prestanda/Monitoring of performance
- ☐ Individuell coaching/Individual coaching
- ☐ Träningsplaner/Exercise plans
- ☐ Annat ...

Hur ofta använder du träningsappar? *
English:
How often do you exercise using fitness apps?

- [ ] Varje dag
- [ ] Minst en gång i veckan
- [ ] Minst en gång i månaden
- [ ] Minst en gång om året

Jämfört med riskerna med att min information avslöjas är användningen av träningsappar fördelaktig för mig. **English:** *
Compared to the risks of my information disclosure, the use of fitness apps is beneficial to me.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jämfört med den information jag behöver avslöja erbjuder användningen av träningsappar värde för mig. *
English:
Compared to the information I need to disclose, the use of fitness apps offers value to me.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Sammantaget levererar användningen av träningsappar ett bra värde för mig. *
English:
Overall, the use of fitness apps delivers good value to me.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är orolig att min information som samlats in av träningsappar kan missbrukas. *
English:
I am concerned that my information collected by fitness apps could be misused.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är orolig över att tillhandahålla min information till träningsappar eftersom den kan användas på ett sätt jag inte förutsåg. *
English:
I am concerned about providing my information to fitness apps because it could be used in a manner I did not foresee.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är orolig över att lämna information till träningsappar på grund av vad andra kan göra med den. *

English:
I am concerned about submitting information to fitness apps because of what others might do with it.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är benägen att avslöja min information genom att använda träningsappar. *

English:
I am likely to disclose my information by using fitness apps.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är intresserad av att avslöja min information till träningsappar. *
English:
I am interested in disclosing my information to fitness apps.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag avser att fortsätta tillhandahålla min information. **English:** *
I intend to continue to provide my information.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är villig att avslöja min information för att fortsätta använda träningsappar. *
English:
I am willing to disclose my information to continue use of fitness apps.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Träningsappar är mycket användbar för min träning. **English:** *
Fitness apps are very useful to my exercise.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Träningsappar tillhandahåller mycket användbar service och information till mig. *
English:
Fitness apps provides very useful service and information to me.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Att använda träningsappar förbättrar kvaliteten på träningen. *
English:
Using fitness apps improves the quality of the exercise.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är orolig att träningsappar kan använda min information för andra ändamål utan att meddela mig eller be om min tillåtelse. * **English:** I am concerned that fitness apps may use my information for other purposes without notifying me or asking for my authorization.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

När jag ger min information till träningsappar är jag orolig att den kan använda min information för andra ändamål. **English:** * When I give my information to fitness apps, I am concerned that it may use my information for other purposes.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Jag är orolig att träningsappar kan dela min information med andra utan att erhålla min tillåtelse. *

English:
I am concerned that fitness apps may share my information with others without obtaining my authorization.

- [ ] Instämmer inte alls - Strongly disagree
- [ ] Instämmer delvis - Disagree
- [ ] Neutral
- [ ] Håller delvis med - Agree
- [ ] Instämmer i hög grad - Strongly agree

Appendix 2 – AI-redogörelse

I arbetet med vår kandidatuppsats har vi använt oss av artificiell intelligens för att effektivisera och hjälpa vår forsknings- och skrivprocess. Trots de många fördelarna som AI erbjuder, är det viktigt att vara medveten om och kritisk till de potentiella riskerna som kommer med användningen.

(Cotton et al., 2023) diskuterar att en risk med att använda AI är dess möjlighet att generera felaktiga eller missvisande uppgifter. Trots sin kapacitet att bearbeta och generera information baserat på stora datamängder, saknar AI förmågan att självständigt verifiera riktigheten i den information som genereras. Detta kan leda till spridning av felaktiga uppgifter, vilket är särskilt riskabelt i arbeten där noggrannhet är avgörande. Dessutom kan användning av AI i forskningsprocessen minska den egna kritiska granskning och djupare förståelse av ämnet. Det är viktigt att kunna balansera användningen av AI-verktyg med traditionella forskningsmetoder och att alltid kritiskt granska och bedöma den information som AI genererar.

De två verktyg som vi har använt oss av är ChatGPT samt Consensus.

Vi har använt ChatGPT, vilket har haft en betydande inverkan på formuleringen av forskningsfrågor och skapandet av innehåll för vår litteraturgenomgång. Dess förmåga att generera information från inmatad data har varit hjälpsam för att utveckla idéer, formulera och finslipa texter samt för att förklara komplexa teorier på ett lättförståeligt sätt. Vi har även använt ChatGPT till att generera kod till pythonscript för att utföra analys på insamlade data.

Consenus, ett plugin till ChatGPT som är ansluten med en stor forskningsdatabas, har visat sig vara ett värdefullt verktyg för att identifiera och granska relevant litteratur. Verktyget ger även information om antalet citeringar en källa har fått och vilka som har citerat den

Referenser

Abdelhamid, M. (2021). Fitness Tracker Information and Privacy Management: Empirical Study. Journal of Medical Internet Research, 23.Tillgänglig online: https://doi.org/10.2196/23059. [Hämtad 10 maj 2024]

Bajpai, A., Jilla, V., Tiwari, V.N., Venkatesan, S.M. and Narayanan, R. (2015). Quantifiable fitness tracking using wearable devices. IEEE Xplore. Tillgänglig Online: doi:https://doi.org/10.1109/EMBC.2015.7318688. [Hämtad 10 maj 2024]

Bhatia, J. and Breaux, T.D. (2018). Empirical Measurement of Perceived Privacy Risk. ACM Transactions on Computer-Human Interaction, 25(6), pp.1–47. Tillgänglig Online: doi:https://doi.org/10.1145/3267808. [Hämtad 2 maj 2024]

Boise, L., Wild, K., Mattek, N., Ruhl, M., Dodge, H.H. and Kaye, J. (2013). Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring. Gerontechnology, 11(3). Tillgänglig Online: doi:https://doi.org/10.4017/gt.2013.11.3.001.00 [Hämtad 23 april 2024]

Brakemeier, H., Widjaja, T. and Buxmann, P. (2016). Association for Information Systems AIS Electronic Library (AISeL) calculating with different goals in mind - the moderating role of the regulatory focus in the privacy calculus. Tillgänglig Online: https://web.archive.org/web/20200323043529id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1115&context=ecis2016_rp [Hämtad 8 maj 2024]

Brough, A.R. and Martin, K.D. (2020). Consumer Privacy During (and After) the COVID-19 Pandemic. Tillgänglig Online: https://www.researchgate.net/publication/341715223_Consumer_Privacy_During_and_After_the_COVID-19_Pandemic [Hämtad 13 mars 2024]

Bui, J. (2016). Lack of Privacy Regulations in the Fitness and Health Mobile App Industry: Assessing the Health Insurance Portability and Accountability Act (HIPPAA) for Meeting the Needs of User Data Collection, Intellectual Property and Technology Law Journal, vol. 21, no. 1, s. 1-20. [Hämtad 23 april 2024]

Chen, H., Gu, Y., Wang, P., Dong, J. and Ren, Y. (2021). Research on Privacy Data Protection in Mobile Applications. Tillgänglig Online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9602169. [Hämtad 26 mars 2024]

Cho, J.Y., Ko, D. and Lee, B.G. (2018). Strategic Approach to Privacy Calculus of Wearable Device User Regarding Information Disclosure and Continuance Intention. KSII Transactions on Internet and Information Systems, 12(7). Tillgänglig Online: doi: https://doi.org/10.3837/tiis.2018.07.020. [Hämtad 10 april 2024]

Christmann, A., & Aelst, S. (2006). Robust estimation of Cronbach's alpha. Journal of Multivariate Analysis, 97, 1660-1674. Tillgänglig Online: https://doi.org/10.1016/J.JMVA.2005.05.012. [Hämtad 10 maj 2024]

Cloudian (2022). Data Protection and Privacy: Definitions, Differences, and Best Practices. Tillgänglig Online: https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/. [Hämtad 26 mars 2024]

Cotton, D., Cotton, P. and Shipway, J.R. (2023). Chatting and Cheating. Ensuring academic integrity in the era of ChatGPT. Chatting and Cheating. Ensuring academic integrity in the era of ChatGPT. Tillgänglig Online: doi:https://doi.org/10.35542/osf.io/mrz8h. [Hämtad 11 maj 2024]

Curry, D. (2024). Fitness App Revenue and Usage Statistics (2024). Tillgänglig Online: https://www.businessofapps.com/data/fitness-app-market/ [Hämtad 12 maj 2024]

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Inf. Syst. Res., 17, 61-80. Tillgänglig online: https://doi.org/10.1287/isre.1060.0080. [Hämtad 23 april 2024]

Eckel, C. and Grossman, P. (2008). Men, Women and risk aversion: Experimental Evidence. Tillgänglig Online: doi:https://doi.org/10.1016/S1574-0722(07)00113-8. [Hämtad 23 april 2024]

Fung Global Retail & Technology. (2017). Percentage of the global population that used a mobile app or fitness tracking device to track their health as of 2016, by age. Tillgänglig Online: https://www-statista-com.ludwig.lub.lu.se/statistics/742448/global-fitness-tracking-and-technology-by-age/ness-tracking-and-technology-by-age/ [Hämtad 2 maj 2024]

Hamed, A. and Ayed, H. (2016). Privacy Risk Assessment and Users' Awareness for Mobile Apps Permissions.Tillgänglig Online: https://ieeexplore.ieee.org/document/7945694 [Hämtad 10 april 2024]

Harris, C.R. and Jenkins, M. (2006). Gender Differences in Risk Assessment: Why do Women Take Fewer Risks than Men? Judgment and Decision Making, 1(1), pp.48–63. Tillgänglig Online: doi:https://doi.org/10.1017/s1930297500000346 [Hämtad 23 april 2024]

Higgins, J.P. (2016). Smartphone Applications for Patients' Health and Fitness. The American Journal of Medicine. Tillgänglig Online: https://www.amjmed.com/article/S0002-9343(15)00537-9/fulltext. [Hämtad 4 april 2024]

Integritetsskyddsmyndigheten (2024). Grundläggande principer. Tillgänglig Online: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/ [Hämtad 19 Mars 2024]

Integritetsskyddsmyndigheten (2021). Känsliga personuppgifter och GDPR. Tillgänglig Online: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/ [Hämtad 19 Mars 2024]

Insight Intelligence. (2018). Delade Meningar - Svenska folkets attityder till digital integritet. [online] Tillgänglig Online: https://dfs.se/delade-meningar/ [Hämtad 12 Mars 2024]

IS Theory (n.d.). Privacy Calculus Theory. Tillgänglig Online: https://is.theorizeit.org/wiki/Privacy_Calculus_Theory [Hämtad 17 april 2024]

Jacobsen, D. I. (2002). Vad, Hur och Varför? Om metodval i företagsekonomi andra samhällsvetenskapliga ämnen. Tillgänglig Online: Ekonomihögskolans biblioteks webbsida http://www.lusem.lu.se/library [Hämtad 28 Mars 2024]

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). Death to the Privacy Calculus?. Innovation Law & Policy eJournal. Tillgänglig online: https://doi.org/10.2139/ssrn.2923806. [Hämtad 28 april 2024]

Lakshman, M., Sinha, L., Biswas, M., Charles, M. and Arora, N.K. (2000). Quantitative Vs Qualitative Research Methods. The Indian Journal of Pediatrics, 67(5), s.369–377. Tillgänglig Online: https://pubmed.ncbi.nlm.nih.gov/10885211/ [Hämtad 28 mars 2024]

Lindskog, E., Huuva, L., Lehtinen, S. and Shannon, D. (2022). Polisanmälda dataintrång: Karriär, utmaningar och utvecklingsområden. Tillgänglig Online: https://bra.se/publikationer/arkiv/publikationer/2022-10-31-polisanmalda-dataintrang.html [Hämtard 9 april 2024]

Majumdar, A., & Bose, I. (2015). Privacy Calculus Theory and Its Applicability for Emerging Technologies., https://doi.org/10.1007/978-3-319-45408-5_20. 191-195. Tillgänglig online: [Hämtad 17 april 2024]

Mitschang, B. and Stach, C. (2014). Design and Implementation of the Privacy Management Platform. 2014 IEEE 15th International Conference on Mobile Data Management. Tillgänglig Online: https://ieeexplore.ieee.org/abstract/document/6916905 [Hämtad 17 april 2024]

Oates, J., Griffiths, M., McLean, R. (2006). Researching Information Systems and Computing, 2e uppl, London: SAGE [Hämtad 2 maj 2024]

Pandey, S. (2020). Principles of Correlation and Regression Analysis. Journal of the Practice of Cardiovascular Sciences, 6(1), p.7. Tillgänglig Online: doi:https://doi.org/10.4103/jpcs.jpcs_2_20f [Hämtad 23 april 2024]

Säkerhetskollen (n.d). Årsstatistik dataintrång 2022. Tillgänglig Online: https://sakerhetskollen.se/brottsstatistik/statistik-dataintrang-2022 [Hämtad 12 april 2024]

Schomakers, E.-M., Lidynia, C. and Ziefle, M. (2021) 'The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance', International Journal of Human-Computer Interaction, 38(13), s. 1276–1289. Tillgänglig Online: https://www.researchgate.net/publication/356539365_The_Role_of_Privacy_in_the_A

cceptance_of_Smart_Technologies_Applying_the_Privacy_Calculus_to_Technology_Acceptance [Hämtad 3 maj 2024]

Shah, A., Banakar, V., Shastri, S., Wasserman, M. and Chidambaram, V. (2019). Analyzing the Impact of {GDPR} on Storage Systems. Analyzing the Impact of GDPR on Storage Systems. Tillgänglig Online: https://www.usenix.org/conference/hotstorage19/presentation/banakar. [Hämtad 22 mars 2024]

Stach, C. (2018). Big Brother is Smart Watching You - Privacy Concerns about Health and Fitness Applications. Proceedings of the 4th International Conference on Information Systems Security and Privacy. Tillgänglig Online: doi:https://doi.org/10.5220/0006537000130023 [Hämtad 17 april 2024]

Statista 2024). Shibboleth Authentication Request. Tillgänglig Online: https://www-statista-com.ludwig.lub.lu.se/outlook/hmo/digital-health/digital-fitness-well-being/health-wellness-coaching/fitness-apps/europe#analyst-opinion [Hämtad 12 mars 2024]

Statistiska Centralbyrån. (2023). Folkmängd efter kön och år, Tillgänglig Online: https://www.statistikdatabasen.scb.se/pxweb/sv/ssd/START__BE__BE0101__BE0101A/BefolkningNy/?loadedQueryId=129324&timeType=top&timeValue=1 [Hämtad 12 april 2024]

Sullivan, G.M. and Artino, A.R. (2013). Analyzing and Interpreting Data From Likert-Type Scales. Journal of Graduate Medical Education, 5(4), pp.541–542. Tillgänglig Online: doi:https://doi.org/10.4300/jgme-5-4-18. [Hämtad 19 april 2024]

Yang, H., Yu, J., Zo, H. and Choi, M. (2016). User acceptance of wearable devices: An extended perspective of perceived value. Telematics and Informatics, 33(2), pp.256–269. doi: Tillgänglig Online: https://doi.org/10.1016/j.tele.2015.08.007. [Hämtad 29 april 2024]

Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A. and Ziefle, M. (2017). Online Privacy Perceptions of Older Adults. Human Aspects of IT for the Aged Population. Applications, Services and Contexts, pp.181–200. Tillgänglig Online: doi:https://doi.org/10.1007/978-3-319-58536-9_16 [Hämtad 23 april 2024]

Zimmer, M., Kumar, P., Vitak, J., Liao, Y. and Chamberlain Kritikos, K. (2018). 'There's nothing really they can do with this information': unpacking how users manage privacy boundaries for personal fitness information. Information, Communication & Society, 23(7), s.1020–1037 Tillgänglig Online: doi:https://doi.org/10.1080/1369118x.2018.1543442 [Hämtad 10 april 2024]