LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Reward Attention

Förslag till ett integritetsdesignmönster

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Linus Nilsson
Jonas Werne
Victor Lindstrand

Handledare: Markus Lahtinen

Rättande lärare: Benjamin Weaver

Osama Mansour

Förord

Vi vill tacka Nick Doty och Miranda Kajtazi, för att de ställde upp och utvärderade vårt integritetsdesignmönster. Vi vill framförallt tacka vår handledare, Markus Lahtinen, som har kommit med värdefulla råd och feedback genom vår skrivprocess.

Maj, 2019

Linus, Jonas och Victor

Reward Attention: Förslag till ett integritetsdesignmönster

ENGELSK TITEL: Reward Attention: Proposal for a privacy pattern

FÖRFATTARE: Linus Nilsson, Jonas Werne och Victor Lindstrand

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Christina Keller, Professor

FRAMLAGD: maj, 2020

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 51

NYCKELORD: Reward Attention, Privacy Pattern, integritet, kryptovaluta, nyttopollett, viewrate,

SAMMANFATTNING (MAX. 200 ORD):

Denna uppsats syftar till att utvärdera ett förslag till ett integritetsdesignmönster. Utvärderingen sker genom att samla in litteratur som rör integritetsfrågor och fenomen för att se vilka faktorer som är relevanta att ta i beaktande för vårt mönster. Den empiriska delen av uppsatsen består sedan av utvärderingar från personer som har en expertis i integritetsfrågor. I mötet mellan litteraturen och utvärderingarna från våra intervjupersoner fick vi nya perspektiv och vinklar att se vårt mönster på, något som presenteras i diskussionskapitlet. Vi har därefter utformat en ny version av vårt ursprungliga mönster, återfinns som bilaga, och presenterat både i utvärderingsdelen och i slutsatsen vad vi har ändrat på och varför.

Innehåll

1 Introduktion

Användning av digitala plattformar är en essentiell del av en majoritet av världens befolkning. Man lever inte bara ett fysiskt liv utan man har ett parallellt liv ute på digitala plattformar, samhället består av en fysik och en digital värld som lever i symbios. Det fysiska samhället har under hundratals år utvecklats och har skapat de grundläggande rättigheter och skyldigheter som alla lever efter. Vad som inte är tydligt är om vi har samma åsikter kring våra rättigheter i den fysiska världen som vi har i den digitala världen.

En majoritet av svenska befolkningen tycker inte att kameraövervakning i offentliga eller allmänna platser är integritetskränkande (Lahtinen, 2019). Människor i Sverige tycker att risken för integritetsintrång är som störst vid dokumentation av en som individ som företag erhåller. Detta kan vara datainsamling som rör individens konsumtionsbeteenden vid online-köp eller närvaro eller vanor på internet och sociala medier (Lahtinen, 2019).

Med ovanstående i beaktning skulle man kunna ponera att människor i Sverige generellt accepterar övervakning av sin person, sin plats, sina vanor vid vad som kan betraktas som offentlig eller allmänna platser och ytor. Internet och sociala medier skulle också kunna tolkas som allmänna och offentliga platser, fast digitala sådana. Dock ska det påpekas att de frågor som ställs om upplevda integritetskränkande övervakning rör specifikt kameraövervakning och inte den typen av datainsamling av individers vanor och tycken, som denna uppsats bland annat berör.

Internet ger möjligheten till tillgång, kommunicering och manipulering av information direkt från alla delar av världen. Den delen av internet som tillgängliggör en stor skara information till varje individ, med en internetuppkoppling och en enhet att koppla upp sig på, är idag till synes gratis för den enskilda användaren att bruka. Dock är det inte gratis för det företaget som är den som erbjuder tjänsten eller produkten. Serverutrymme, datorer, utvecklare, kundtjänst, marknadsföring – listan kan göras lång och få saker på listan är gratis. Således måste företagen som erbjuder gratis tjänster eller produkter få in intäkter på annat vis än direkt från sina respektive användare. Exempelvis Google låter, simpelt uttryckt, annonsörer buda mot varandra för att deras annonser ska komma högre upp i sökresultaten för användare (E. Rosenberg, 2018). Högre bud visas högre upp i resultaten, medan lägre bud kanske inte visas överhuvudtaget. Annonsörerna betalar sedan Google varje gång en besökare klickar på deras annons. Användarklicken varierar i värde beroende på vad annonsernas innehåll och hur vanliga sökorden är (E. Rosenberg, 2018).

Denna lösning är dock inte helt utan problem, risker eller eftergifter. Respektive användare måste exempelvis göra eftergifter när det kommer till annan parts tillgång till deras personliga information i form av preferenser och beteenden i den digitala sfären. Det är nämligen endast genom att logga hur användare agerar på internet som företag som exempelvis Google kan rikta rätt annons till rätt målgrupp. Detta är en eftergift som många människor gör, både medvetet och omedvetet, dagligen genom att besöka hemsidor, genom att använda vissa tjänster och vissa produkter – i de fall som det är medvetet förekommer det också vanligtvis en motivering till varför den eftergiften är värd att göra. Oaktat om denna eftergift görs medvetet eller omedvetet så ligger det ett tungt ansvar på företagen som har fått förtroendet att hantera dessa

människors digitala avtryck – det är nämligen dem som måste säkerställa att det används som överenskommet och att ingen obehörig part får tillgång till informationen.

Vanligtvis flyter denna överenskommelse på utan några märkbara problem trots hotbilder i form av exempelvis dataintrång eller att information på något annat sätt hamnar i fel händer. Menat att användarna känner sig trygga i att deras information används på ett lämpligt och överenskommet sett. De får fortsatt gratis tillgång till exempelvis sökmotorer eller andra jämförbara tjänster eller produkter, och företagen som erbjuder nämnd tjänst eller produkt kan fortsätta locka till sig annonsörer. Detta bland annat på grund av diverse säkerhetssystem och säkerhetsåtgärder främst från företagens sida.

1.1 Integritetshaverier & dataintrång

Det har dock inträffat integritetshaverier genom tiderna som avsevärt påverkat förtroendet för individuella företag och påverkat trovärdigheten för deras förmåga att skydda och hantera människors personliga data. För ett par år sedan så hade ett dataintrång som potentiellt kunde påverka ett par miljoner användare varit stora nyheter. Idag är det allt vanligare att dataintrång påverkar hundratals miljoner (Swinhoe, 2020). Vidare är det inte bara dataintrång som är den enda hotbilden, utan det kan även vara en anställds borttappade laptop, telefon eller USB-drive – dessa är också integritetshaverier. Företag och organisationer förstår mångt och mycket riskerna i att en laptop som innehåller potentiellt känsliga data blir antingen borttappad, bortglömd eller bestulen, men samma riskförståelse finns inte alltid när det kommer till portabla datalagringsenheter. USB-drives, externa hårddiskar eller en laptop som glöms bort på sätet i en bil är en enorm risk. Företagen *Home Depot* och *Pfizer* har båda fått problem när laptops som innehåll känslig data blev stulna (Vance, 2008). Om det inte säkerställs på förhand att potentiellt känsliga data, eller nycklar som exempelvis lösenord eller annat dylikt som används för att få tillgång till data, är det nästan omöjligt att vara helt skyddad mot tjuvar eller helt enkelt glömska från ens egna anställda.

1.1.1 Stulna kredikortsuppgifter

Adobe är ett programvaruföretag som idag främst fokuserar på redigering och publicering av trycksaker och grafik. De har även olika lösningar för företag, exempelvis signeringslösningar som *Adobe Sign* som accepteras juridiskt världen över.

Det inträffade ett dataintrång hos *Adobe* i oktober 2013 där hackare stal uppskattningsvis 3 miljoner kundkredikortsposter och inloggningsdetaljer för ett obestämbart antal användarkonton. Vid ett senare datum samma månad rapporterade *Adobe* själva att uppskattningen inkluderade nu även ID:s och krypterade lösenord för 38 miljoner aktiva användare. En fil som förmodas ha postats av någon involverad hackare, inkluderade över 150 miljoner användarnamn och lösenordspar tagna från Adobe. Något annat som också stals i dataintrånget var delar av källkod för *Adobe Acrobat* och för deras *Cold Fusion* webapplikationsplattform (Krebs, 2013).

Adobe blev i november 2015 tvungna att betala 1,1 miljoner dollar i juridiska kostnader och totalt 1 miljon dollar till påverkade användare för anklagande om lagstiftningsbrott och för orättvisa affärsmetoder (Krebs, 2013).

1.1.2 Stulna användarkonton och undanröjd sökningshistorik

Yahoo är företag som erbjuder en rad olika tjänster och produkter som exempelvis *Flickr* och *Tumblr*, men som är mest kända för sin söktjänst *Yahoo!*

Yahoo avslöjade i september 2016 att företaget år 2014 hade varit offer för ett enormt dataintrång. Hackarna, fick tillgång till namn, mailadresser, födelsedatum och telefonnummer för över 500 miljoner användare. Yahoo menade på att majoriteten utav lösenorden som stals var hashade (Williams, 2017).

I december 2016 avslöjade Yahoo att ett annat dataintrång hade inträffat år 2013 av en annan hackare, som fick tillgång till namn, födelsedatum, mailadresser, lösenord och användares valda säkerhetsfrågor och svar på dem frågorna för över 1 miljard användarkonton. Yahoo reviderade sedan den uppskattningen oktober 2017 och inkluderade alla deras 3 miljarder användarkonton i uppskattningen (Swinhoe, 2020).

1.2 Felaktig användning av personliga data

Besökare av digitala och analoga affärer och varuhus delar endast med sig utav sina pengar. Åtminstone såvitt besökarna vet, men vad de också delar med sig, potentiellt omedvetet, är deras köpvanor och köpmönster. Dessa vanor och mönster har åtminstone *Target* tagit del av och använder informationen för att klura ut med hjälp av algoritmer vilka rabatter och kuponger som var enskild kund hade varit intresserad utav. *Target* har dock tagit det ett steg längre, nämligen till att försöka förutspå förändringar i deras kunders liv och därefter vilka produkter som de hade varit intresserade av att köpa innan kunden själv vet det (Hill, 2012).

År 2012 offentliggjordes det att *Target* och dess algoritm hade räknat ut att en kund var gravid baserat på köpvanor och köpmönster långt innan kunden visste det och började erbjuda kuponger i förväg (Hill, 2012).

Det finns en annan risk med när företag förlitas på att hantera människors personliga data på ett schysst sätt. Nämligen risken att företagen inte är helt transparenta med de olika sätt som de använder data på. Ett potentiellt exempel på det är hur Google hanterar och processar sina användares platsdata, något som Irlands dataskyddskommission nu undersöker för brott mot rådande GDPR-lagstiftning efter att en rad olika företag, tjänstemän och akademiker runt om i Europa anmält Google (Birnbaum, 2019). Google har å sin sida har sagt att de mer än gärna samarbetar och att de vill att människor ska förstå och kunna kontrollera hur företag som Google använder platsdata för att erbjuda dem olika tjänster (Birnbaum, 2019).

Google använder ett system för att släppa ut personlig information om deras användare till externa företag, det påstår i alla fall rivaliserande webbläsaren Brave. De menar att Google använder sig av webbsidor som kallas för ”push-sidor” som då kan dela användarinformation till en tredje part som exempelvis ett annat företag. Google däremot säger att de inte visar personliga annonser eller skickar anbudsförfrågningar till anbudsgivare utan att respektive användare har givit sitt samtycke att så får lov att ske (Birnbaum, 2019).

1.3 Kapprustning

Med ovanstående exempel i beaktning är det inte konstigt att människor blir oroliga över deras personliga integritet och över hur deras personliga data hanteras av diverse företag. När användare inte längre förlitar sig på att företagen vars tjänster de använder hanterar deras personliga data på ett överenskommet och säkert sätt, så ser de kanske till vilka verktyg de själva kan använda sig utav för att skydda sin data eller begränsa andra parters tillgång till den. Ett exempel på ett sådant verktyg är annonsblockering.

Annonsblockering kan, från en internetanvändares perspektiv användas av ett flertal olika anledningar. Integritetsskydd, skydd mot skadliga annonser som popupfönster eller auto-dirigeringar. Oaktat anledningen så finns det klara fördelar för användaren, men vi menar att det också kan finnas framtida potentiella konsekvenser om användandet av annonsblockering blir utbrett. Några utav fördelarna för användaren webbsidor som laddar snabbare och med färre saker på sidan som distraherar. Då exempelvis de sökmotorer som finns får intäkter genom annonsering så behöver man inte tänka alltför länge vad ett potentiellt resultat skulle vara om annonsblockering blir alltmer utbrett bland internetanvändare världen över. Det ska dock nämnas att hemsidor kan ta motåtgärder mot annonsblockering genom att försöka upptäcka om besökaren har en annonsblockerare aktiv och informera besökaren om hur det påverkar hemsidans fortsatta existens. En annan motåtgärd är att blockera besökare från att använda sidan tills det att de avaktiverar deras annonsblockerare.

1.4 Reform

> *Surveillance capitalism is about to become obsolete, the Irish Data Protection Commission's action signals that now – nearly one year after GDPR was introduced – a change is coming that goes beyond just Google. We need to reform online advertising to protect privacy, and to protect advertisers and publishers from legal risk under the GDPR.*
> (Ryan, 2019)

Istället för att kapprustningen mellan annonsblockerare och åtgärder mot dem annonsblockerarna ska fortgå, så borde det istället tittas på om det finns en lösning i hur vi designar våra system och hur de förhåller sig till människors syn på sin integritet på internet. Ett sådant försök är Privacy Patterns (integritetsdesignmönster), som ämnar att formalisera designlösningar på vanliga digitala integritetsproblem. Detta är ett sätt att standardisera terminologier, vanliga arbetsmetoder, bästa praxis och göra allt tillgängligt för utvecklare världen över så att de kan bättre tackla integritetsproblem redan i hur de designar sina system, tjänster och produkter.

1.5 Forskningsfråga

Utvärdera ett förslag till ett integritetsdesignmönster.

1.6 Syfte

Vårt syfte med denna uppsats är att bidra med ett mer integritetsvänligt alternativ till hur man kan bedriva digital annonsering genom att skapa ett integritetsdesignmönster. Vidare är syftet

att skapa ett designmönster som kan förbättra redan existerande systemen för att förenkla för framtida utvecklare som vill dra nytta av en sådan design. Designmönster av denna typ kan liknas metoder, eller verktyg, och syftet med uppsatsen är därmed att bidra med en metod för att tackla integritetsproblem i designfasen för utvecklare.

1.7 Avgränsningar

Vi tar inte i uppsatsen hänsyn till den potentiellt drastiska omställningen som diverse företag hade varit tvungna att göra för att kunna implementera detta designmönster. Vi tar i uppsatsen inte hänsyn till användarens perspektiv vid utformningen av designmönstret, utan vi riktar oss främst till utvecklare. Vidare kommer vi inte att fokusera på hur vi skapade vårt initiala mönster, utan meningen med uppsatsen är att utvärdera ett mönster vi skapat innan. Slutligen lägger vi inget fokus vid reklam eller annonser som fenomen och inte heller vid de olika typer av reklam och annonser som finns.

2 Bakgrund

I denna del kommer den teori som ligger bakom undersökningen presenteras. Litteraturen är uppdelad i tre olika kategorier: integritet, Privacy Patterns och online-annonsering. Vi börjar med att förklara och definiera integritet följt av en djupare genomgång om Privacy by design och Privacy Patterns. Avslutningsvis presenterar vi hur online-annonsering fungerar tillsammans med annonsblockering, decentraliserad annonsering och hur vi definierar begreppet view-rate.

2.1 Integritet

2.1.1 Digital Integritet

För att kunna diskutera ämnet integritet så måste man veta vad integritet faktiskt är. Svenska Akademins ordbok definierar integritet som: ”*rätt att ha en egen sfär som är skyddad mot intrång*” (Svenska Akademins Ordböcker, 2015). När det kommer till digital integritet så gäller det att man har rätt till att vara skyddad från intrång på digitala plattformar som på internethemsidor. Ytterligare så definierar nya dataskyddsförordningen (GDPR) att det är personuppgifter ska som skyddas (Datainspektionen, n.d.). Personuppgifter definierar Datainspektionen som information som kan på något sätt kan knytas tillbaka till en person.

Ytterligare så har Holvast (1993) och Rosenberg (1992) kommit fram till tre olika aspekter av integritet. Första är territoriell integritet innefattar att har integritet i ett fysiks sammanhang, en plats som folk inte ska få tillgång till utan tillåtelse exempelvis ens hem. Den andra typen av integritet är person integritet, att fysiskt röra och söka en person kan kränka denna typ av integritet. Denna uppsats kommer att behandla den tredje och sista typen av integritet som är informativ integritet. Den behandlar personlig data och hur den samlas, behandlas och lagras. När integritet nämns i denna uppsats så är det informativ integritet som menas.

En artikel av Tene och Polonetsky (2013) så lyfter man fram att ett legalt ramverk måste upprättas för vi har ett behov att reglera vad som verksamheter får och inte får lov att göra med den data som vi användare skapar. Sedan denna artikel skrevs så har GDPR upprättas i Europa men det är fortfarande ett diffust ämne. Vad som är och inte är en personuppgift anses vara oklart (Tene & Polonetsky, 2013). Personnummer är lätt att förstå att det är en personuppgift men sökhistorik känns inte som en personuppgift. Men om man observerar tillräckligt mycket data så kommer mönster uppstå i sökhistoriken som kan kopplas med användaren. Har någon sökt efter en kaffekokare och du har sökt efter gym så kan man knyta ihop med en person som precis har köpt en ny kaffekokare och har köpt ett nytt gymmedlemskap. På ytan så är inte sökhistorik en personuppgift men om man har tillräckligt mycket användardata så kan det diskuteras att sökhistorik är en personuppgift.

2.1.2 Integritetsetik

Men varför bör man skydda sin integritet? Man hade kunnat argumentera att integritet inte bör skyddas och därav finns det inget behov av ett integritetsmönster. God eller bristande integritet är kopplat till vad som är etiskt rätt eller fel (Moor, 1990). Lagar reflekterar vad samhället anser vara rätt eller fel, men på grund av den hastigheten som teknologin utvecklas så blir det allt svårare att reglera eftersom lagstiftningsprocessen tar lång tid.

Vilka integritetsval som användare gör bör i någon mån grunda sig i de etiska grundprinciper varje individ lever efter. Hur användarnas data behandlas och hur data sparas idag ligger i konflikt med etiska grundprinciper. Därav så kan det fastställas att det finns ett problem när integritet kränks. Om etiska principer aktivts används så bör man ta några åtgärder till de risker som finns. När man designar ett system så bör man ur ett etiskt perspektiv följa vissa grundprinciper i designen för att man ska utforma ett etiskt system.

Jeroen Van den Hoven (2008) beskriver fyra olika etiska anledningar till att man bör skydda sin integritet. Först nämner han informationsbaserad skada, personlig data som sparas i någon form av databas vilket skapar en risk för intrång. Den potentiella risken för att något kan hända är tillräckligt för att man ska vidta åtgärder för att förhindra att något sådant kommer ske.

Den andra anledningen handlar om informationsbaserad ojämställdhet. Med detta menar Van den Hoven att den information som vi ger till företag har ett stort värde, men användare har ingen möjlighet till rättvis kompensation. Det gör att företagen får mer och mer makt över användarna (Van den Hoven, 2008). Till exempel om en tjänst har en annonsplats på deras hemsida och de samlar information om deras användare för att rikta annonser till dem. Då är detta oetiskt då man kränker användarens integritet för att som tjänst kunna tjäna mer pengar.

Tredje anledningen är informationsbaserad orättvisa, när vi ger ut vår personliga data så förutsätter vi att den informationen enbart ska användas inom samma kontext som den samlats in (Van den Hoven, 2008). Till exempel den information som samlas in på ett sjukhus ska bara användas inom sjukvården. När information säljs mellan företag så utnyttjas din information i andra kontexter än vad den var ämnad till och därmed på ett orättvist sätt.

Fjärde och sista anledningen handlar om moralisk autonomi och identifikation. Man bör ha kontroll över hur sina personuppgifter behandlas och vilken data som samlas in (Van den Hoven, 2008). Många internetbaserade tjänster skapar profiler av användare, genom att inte ge användaren direkt kontroll över sina profiler, så överensstämmer dessa sällan med hur användaren identifierar sig själv.

2.1.3 Integritetssegmentering

Vi har ovan definierat vad integritet är samt nämnt etiska argument till varför människor bör skydda sin integritet. Alla människor har dock inte samma etiska och moraliska grundprinciper när det gäller integritet. Alan Westins integritetssegmenteringteori delar i allmänhetens syn på integritet i tre olika grupper: (1) Fundamentalister, (2) Pragmatiker och (3) Obekymrade (Kumaraguru & Cranor, 2005). Akademiker från en rad olika discipliner har under många år använt Westins integritetssegmenteringsteori för att göra integritetsanalyser (Hoofnagle & Urban, 2014). Westins integritetssegmenteringsteori har förvisso fått en del kritik, framförallt att den har metodologiska brister som inte kan fastställa att användare är pragmatiska i vare sig teorin eller i praktiken (Preibusch, 2014; Urban & Hoofnagle, 2014). Vi väljer ändå att använda oss av Westins integritetssegmenteringsteori eftersom den framvisar skillnader i integritetspreferenser.

Fundamentalisterna (1) står får cirka 25% av befolkningen. Denna grupp värdesätter integritet väldigt högt, och anser att fler individer borde vägra att ge ut information som de blir ombedda till. De avvisar att organisationer har behov eller rätt att få tillgång till personlig information för att kunna bedriva sin verksamhet. Fundamentalisterna är för införandet av striktare lagar för att säkerställa integritetsrättigheter och kontroll av organisationers hantering av

personlig data (Westin, 2002 refererad i Urban & Hoofnagle, 2014). Fundamentalister har en generell misstro mot organisationer som samlar in personlig information och är oroliga för precisionen i digital information. Denna person brukar vanligtvis offra saker som annars tenderar till att vara av största vikt såsom effektivitet, låg kostnad, individanpassade tjänster och produkter för att i gengäld skydda sin integritet på ett bättre sätt (Kumaraguru & Cranor, 2005).

Pragmatiker (2) står för cirka 55% av befolkningen. Dessa personer gör en *cost-benefit-analys* där riskerna med att ens personliga data sparas och används, vägs mot de upplevda fördelarna. *Cost-benefit-analysen* resulterar vanligtvis med att man är villig att ta risken eftersom de vill åt fördelarna som tillkommer med att dela sin information online. Dock är personer som ingår i denna grupp inte helt obesvärade när det gäller att ge bort, offentliggöra eller tillgängliggöra sin personliga integritet, eftersom de fortfarande värdesätter integritet. Pragmatikerna föredrar frivilliga standarder och att konsumenter får bestämma själva framför lagstiftning och myndighetsåtgärder. Men de kommer att stödja lagstiftning när de tycker att de blir utnyttjade och att det inte görs tillräckligt för att skydda dem (Westin, 2002 refererad i Urban & Hoofnagle, 2014). Pragmatiker anser att företag eller myndigheter bör "förtjäna" allmänhetens förtroende snarare än att automatiskt anta att de har det. De vill också ha möjlighet att själva få välja hur deras personliga information får hanteras, t.ex. om de ska vara med i företags e-postlistor (Kumaraguru & Cranor, 2005).

Obekymrade (3) står för cirka 20% av befolkningen. Denna grupp vet inte vad "integritets ståhejet" handlar om, och har inga problem med att lämna ut personlig information till myndigheter eller företag och ser inget behov av att skapa ännu mer statlig byråkrati för att skydda någons integritet (Westin, 2002 refererad i Urban & Hoofnagle, 2014). De obekymrade har generellt sett förtroende för organisationer som samlar in personliga information, och är bekväma med de befintliga integritetspolicyn företag har (Kumaraguru & Cranor, 2005).

2.2 Design patterns

2.2.1 Privacy by Design

Målet med *Privacy by design* är att istället för att lösa potentiella integritetsproblem i efterhand så ska god integritet vara en del av systemets design. Genom att följa vissa principer så kan man uppnå ett integritetsvänligt system, dessa sju kärnprinciperna kommer att presenteras nedanför (Davies, 2010).

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default
- Privacy Embedded into Design
- Full Functionality – Positive-Sum, not Zero-Sum
- End-to-End Security – Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy

Enligt *Privacy by Design* bör potentiella integritetsproblem behandlas proaktivt, inte reaktivt. Genom att lösa problemen från grunden i systemets design så kommer man inte få problem i framtida användning av systemet (Davies, 2010). Detta ser till att systemet har integritetsskydd som standard, om en integritetskränkande funktion finns så måste användare aktivera

den själv för att ge användaren valet själv. Detta förhindrar personer som inte vet hur deras data behandlas från att blir utnyttjade genom att skydda deras integritet som standard. Systemen kommer även fungera mer optimalt eftersom integritet inte kommer som en eftertanke så behöver man inte göra restriktioner för funktioner (Davies, 2010). Att följa dessa principer ska ge en positiv effekt för både tjänsten och användarna. Att behöva prioritera integritet över säkerhet ska inte vara nödvändigt utan man kan ha bra fokus på båda.

Varje gång ett system behandlar någon form av data så bör en säker koppling mellan användare och systemet genom att kryptera den informationen så ingen utomstående kan få tillgång till information (Davies, 2010). Detta bör vara inbyggt inom alla delar av databehandlingen. Tillsammans med att allt som ett system gör bör vara transparent för alla dess involverade parterna, genom att vara tydlig med vad som användaren och tjänsten ger i utbytte med varandra så kan en tillit skapas mellan båda parterna. Det som är viktigast är att hålla användarens integritet i huvudfokus, användarna är den centrala delen av varje system.

2.2.2 Privacy Patterns

Privacy by design, det vill säga processen att översätta integritetsproblem till reella tekniska lösningar, har visat sig vara svårt. En samling av ingenjörer, designers, advokater och tillsynsmyndigheter involverade i integritetsfrågor hoppas att introducerandet av *Privacy Patterns* kan förbättra kommunikationen om beprövade metoder, standardisera språket för integritetsskyddande teknologier, dokumentera vanliga lösningar på integritetsproblem samt hjälpa designers att identifiera och hantera integritetsproblem (Privacy Patterns, 2020).

Privacy Patterns är föreslagna designlösningar på vanliga upplevda integritetsproblem (Privacy Patterns, 2020). De är abstrakta praktiska förslag till mjukvarudesign, som exempelvis skydd mot spårning, minimering av datainsamling och distribution samt minimal informationsasymmetri.

Varje *Privacy Pattern* är uppbyggt på ett sätt som ska göra det enkelt att förstå och lätt kunna använda för att utforma system efter dessa mönster (Privacy Patterns, 2020). Varje mönster innehåller en kontext-del, ett integritetsproblem och en lösning över hur man bör gå tillväga för att lösa problemet i systems design. *Privacy Pattern* listar även konsekvenser som kan uppstå tillsammans med ett kort praktiskt exempel samt välkända exempel om det finns.

2.3 Online-annonsering

Online-annonsering, även känt som online-marknadsföring, internetreklam, digital reklam eller webbannonsering, är en form av marknadsföring som använder Internet för att framföra marknadsföring till konsumenter. Likt andra typer av marknadsföring involverar online-annonsering ofta en utgivare, som integrerar annonser i dess online-innehåll, och en annonsör, som tillhandahåller annonserna som ska visas i utgivarens innehåll.

En stor del av webbplatserna på Internet finns tack vare online-annonsering. Miljontals webbplatser, från små bloggar till enorma företagsägda tidskrifter, är beroende av online-annonsintäkter för att kunna fungera och existera (Shewan, 2020). Dagens online-annonsering är de facto lönsam för alla inblandade eftersom utgivare upprätthåller "fri" åtkomst för användare, annonsörer marknadsför produkter och tjänster för att få nya kunder, annonsnätverk samlar

utgivare och annonsörer, och webbplatsbesökare använder annonsvisningar som valuta för tillgång till dess innehåll (Davar, 2013 refererad i Ivanjko & Bezjak, 2017).

En tänkbar baksida med dagens online-annonsering är att utgivare, annonsörer och datamäklare spårar användare på nätet för att erbjuda anpassat innehåll och riktad reklam. Massvis av data samlas in, bearbetas och sammanförs till *Big Data* med målet att tillhandahålla användarnas behov så precist som möjligt. Detta kan verka användarvänligt och renhjärtat men missbruk av data är vanligt, och webbplatser samlar ofta värdefulla personuppgifter från sina besökare för att sälja till tredje part (Searls, 2015). Spårningen online har väckt frågor kring integritet och övervakning eftersom den tillåter annonsörer att använda känslig information om användare såsom deras medicinska och ekonomiska förhållanden (Mayer & Mitchell, 2012). I och med att användardata blir allt mer sofistikerad (Evans, 2009), kan nationalstater utnyttja all den information som samlas in om individer för att utföra massövervakning (Englehardt et al., 2015).

2.3.1 View-rate

Det finns olika sätt att beräkna hur effektiv en online-annons är. Ett vanligt tillvägagångssätt är att använda sig av *click-through rate. Click-through rate* är andelen personer som ser din annons och som sedan faktiskt klickar på annonsen. Genom att använda *click-through rate* mäter man annonsens effektivitet utifrån antalet klick som annonsen får per antal visningar (WordStream, 2020).

För att spåra värdet på videokampanjer använder Youtube begreppet *view-rate. View-rate* definieras som förhållandet mellan antalet visningar för en videoannons och antalet visningar på ett videoklipp. Om du till exempel hade 5 betalda visningar och 1000 visningar skulle din *view-rate* vara 0,5%. *View-rate* liknar *click-through rate*, men istället för att mäta klick, räknar den antal personer som faktiskt har sett en video-annonsen på YouTube (Google, 2020).

I denna uppsats använder vi begreppet *view-rate* som mått på hur effektiv och nyttjad en annons är. Vår definition av *view-rate* skiljer sig från Youtubes, då vi definierar *view-rate* som den sammanställda tid och uppmärksamhet en användare lägger på en annons.

2.3.2 Annonsblockering

Annonsblockerare kan ta bort eller ändra annonsinnehåll från en webbläsare, webbplats eller mobilapp. Människor kan välja att installera annonsblockeringsprogramvara själva, men programvara har också introducerats av vissa webbläsare och mobiloperatörer (IAB UK, 2019). Mer än 750 miljoner enheter använde annonsblockerare i december 2019 (PageFair, 2020) där män mellan 18 och 34 är den typiske användaren (IAB, 2016).

Det finns flera förklaringar till varför man vill använda annonsblockerare, men de främsta skälen till att folk laddar ner annonsblockeringsprogramvara är för att blockera några eller alla annonser, förbättra prestanda eller skydda deras integritet (IAB UK, 2019). Integritetsoro är den mest uttalade invändningen som användare har mot annonsering på nätet, där den bakomliggande anledningen kan tillskrivas felaktig hantering av personuppgifter (PageFair, 2017). Användare känner sig också säkrare att surfa på nätet när de är skyddade från annonser som kan överföra skadlig programvara utan deras godkännande, och de tolererar inte annonser som innehåller falska exit- eller nedladdningsknappar som pressar användare att klicka på dem innan de fortsätter till den önskade sidan (Davar, 2013 refererad i Ivanjko & Bezjak, 2017). Användare tycker även att annonser ofta är störiga och irriterande, där de mest irriterande

annonserna är: annonser som blockerar innehåll, långa videoannonser innan korta videor samt annonser som följer med ner på sidan när användaren scrollar (IAB, 2016).

Forskning visar att konsumenter är trötta på att mer och mer bombarderas med påträngande reklam på nätet (Newman, Levy & Nielsen, 2015). 47% av amerikanerna och 39% av britterna använder sig av annonsblockerare för att slippa se annonser. Mer en tredjedel eller mer säger även att de ignorerar annonser, och cirka tre av tio säger att de aktivt undviker webbplatser där annonser stör innehållet.

2.3.2.1 Problematiken med annonsblockerare

Eftersom utgivare huvudsakligen förlitar sig på annonser för att tjäna pengar på sina tjänster förlorar de intäkter om en besökare använder en annonsblockerare för att ta bort sidans annonser. Annonsblockering beräknades kosta utgivare nästan 22 miljarder dollar i förlorade intäkter under 2015 (PageFair, 2015). Den ökande popularitet för annonsblockering har drivit utgivare till att försöka stoppa annonsblockerings-användare (Iqbal, Shafiq & Qian, 2017).

Vissa menar på att online-annonsering genomgår en existentiell kris. Intäkterna från annonser fortsätter att sjunka och det finns oro i branschen över bedrägeri och brist på insyn (Newman, Levy & Nielsen, 2015). Användare har blivit överväldigade av annonser på nätet, som i sin tur har svarat genom att ta bort annonser med hjälp av annonsblockeringsteknik. Eftersom det mesta av det innehåll som finns tillgängligt online finansieras med reklamintäkter står rätten till ett ”gratis internet” på spel (Ivanjko & Bezjak, 2017). En enskild webbanvändare kan förbättra sin webbupplevelse genom att blockera annonser, men när många användare gör det, kan effekterna på intäkter och investeringar undergräva kvaliteten på det annonsstödda innehållet, vilket kan resultera i att alla användare får sämre innehåll på Internet (Shiller, Waldfogel & Ryan, 2017).

Annonsblockeringstrenden gör att många utgivare överger de gamla modellerna till förmån för sponsrat innehåll. Buzzfeed, Vox, och Vice går i bräschen, och New York Times, Washington Post och Guardian har sammansatt kreativa team för att skapa redaktionellt innehåll tillsammans med företag. Detta är dock ganska kontroversiellt inom branschen eftersom det tenderar att sudda ut gränsen mellan redaktionellt arbete och reklam. Konsumenterna verkar heller inte helt nöjda med denna modell då en tredjedel eller fler säger att de har känt sig besvikna eller lurade efter att ha läst en artikel som de senare fann var sponsrad (Newman, Levy & Nielsen, 2015). Samma studie visar att hälften av deltagarna inte tycker om sponsrat innehåll men accepterar det, medan över en fjärdedel får en försämrad bild av nyhetsorganisationer till följd av sponsrat innehåll. Vidare ger online-annonsering mycket större intäkter än betalväggar (Shiller, Waldfogel & Ryan, 2017).

Ett annat verktyg som utgivare har satt mot annonsblockering är att neka åtkomst till besökare som använder sig av annonsblockerare. En person som använder annonsblockerare möts av två val när den besöker webbplatsen: användaren kan antingen inaktivera sin annonsblockerare, eller ha annonsblockeraren igång och avstå från att besöka webbplatsen. Dock uppger 74% av amerikanska annonsblockerings-användare att de lämnar webbplatser med anti-adblock-väggar (PageFair, 2017).

Kampen som spelas mellan utgivare och annonsblockerare tros komma att ha en stor inverkan på Internet, där annonsblockerare förändrar status quo för annonsdrivet innehåll och tjänster (Iqbal, Shafiq & Qian, 2017). Medan Google har vidtagit åtgärder för att avskräcka

annonsblockering, försöker deras webbläsares konkurrenter att erbjuda annonsblockering som en funktion (PageFair, 2020). Shiller, Waldfogel & Ryan (2017) menar ifall man inte kan ta fram en teknisk lösning till detta dilemma, behöver utgivare försöka utforska möjligheten för en reglering eller lagstiftning mot annonsblockerare.

2.3.3 Decentraliserad annonsering

Integritetsmönstret som har skapats har baserats på ett existerande system som finns i drift. Genom att skapa en abstrakt version så kan denna design användas på ett mer generellt sätt vilket skapar mer integritetsvänlig annonsering. Ett förslag till hur man kan få bättre integritet är decentraliering (Colesky, Hoepman & Hillen, 2016). I kombination med att man ger användaren mer kontroll så kan man skapa den design som förhåller sig till en bättre integritetsstandard.

Normalt så fungerar digital annonsering att hemsidor som publicerar annonser ofta får betalt efter hur effektiv annonserna är. Om användarna inte kan kontrollera hur deras användardata används så ger man inte användaren ett val om deras användardata ska användas till effektiviseringen av annonser. Användardata använder tjänsterna för att försöka matcha annonser med deras användarmönster. Tjänster använder även andra metoder för att få användare att klicka på annonser genom att maskera annonser som genuint innehåll istället för att separera plattformens innehåll och annonser. Exempel på detta är sökresultaten på Google där ofta reklamen är inte går att särskilda från andra sökresultat. Det enda som separera dem är en liten *ad* loga som sitter bredvid men ofta så tänker man inte på detta (se figur 1).

Figur 1. Google sökresultatsexempel

Problemet för tjänsterna är att annonserna får väldigt låg interaktion då många användare väljer att blocka annonser med ad-block mjukvaror. Genom att använda sig av en *opt-in* strategi så kommer att göra digital annonsering mer effektiv då användarna själva har valt att få annonser (Montero, 2000).

Istället för att försöka lura användare med annonser som ser ut som hemsidans vanliga innehåll för att få användarnas uppmärksamhet. Så bör man ge användarna mer autonomi över deras annonseringsval. Som Montero (2000) säger så bidrar en *opt-in* strategi till mer effektiva annonser med högre *view-rate*. Med mer effektiva annonser så behöver tjänsterna inte spendera lika mycket resurser för att ”lura” användarna. Detta system ger en även användarna som konsumerar dessa annonser en form av kompensation för att man har både lagt tid på att se annonser men även att man ge tillgång till ens beteende mönster vilket kan kränga ens integritet ock därav så bör man få något för det.

Det finns exempel på ett sådant system i bruk just nu. Brave är en webbläsare som har skapat ett separat system som gör det möjligt för användare att välja om man vill blocka all annonsering eller få annonser i utbyte mot en kryptovaluta (*BAT*). Pengarna som vanligtvis gick till de

sidor som publicera annonserna delas nu upp till användare och de som publicerar genom kryptovalutan *BAT* (Brave software, 2018). Annonserna distribueras till användaren direkt i webbläsaren, alltså inte på själva hemsidorna.

Användaren skyddas automatiskt genom att både tjänsterna och de som företagen som skapar annonserna inte har tillgång till användardata, BAT fungerar som en medlare mellan alla tre parter vilket förhindra missbruk av användardata (Colesky, Hoepman & Hillen, 2016). Detta skapar ett system som både är mer effektivt men även mer skyddande mellan alla parter.

2.3.4 Sammanfattning

Privacy by design innebär att integritetsskydd tas i beaktning redan när man utformar IT-system och rutiner. På så vis blir integritetsskydd en standard. *Privacy Patterns*, eller integritetsdesignmönster, fungerar som ett stöd till systemdesigners att tillämpa integritetsskyddande åtgärder under hela systemutvecklingens livscykel. Tillämpningen av integritetsdesignmönster ska leda till att användare skyddas och får större kontroll över sin egna data.

Van den Hoven (2008) menar att integritet är något som alla bör skydda. Utnyttjande av användardata är fenomen som sker dagligen och som på många sätt kränker användare utifrån etiska principer. Därav finns det ett behov av att man designar informationssystem med riktlinjer som följer etiska principer. Dock så är inte lätt att avgöra var gränsen går över vad som etiskt rätt eller fel. Varje person har egna etiska principer som de lever efter, och att försöka skydda användares integritet till varje pris är inte helt oproblematisk eftersom användare har olika integritetspreferenser. Utifrån Westins integritetssegmenteringsteori kan man dela in allmänhetens syn på integritet i tre olika grupper: (1) Fundamentalister, (2) Pragmatiker och (3) Obekymrade (Westin, 2002 refererad i Urban & Hoofnagle, 2014). Om man utgår ifrån Westins integritetssegmenteringsteori så uppstår det ett svårt dilemma i att försöka tillfredsställa alla tre gruppers behov och preferenser genom ett integritetsdesignmönster.

Fundamentalisterna (1) blir endast nöjda ifall deras integritet är högsta prioritet. Denna grupp ser alltid till att använda så integritetsfrämjande tjänster som möjligt och kan tänka sig att offra fördelar såsom effektivitet, låg kostnad och individanpassning för att i gengäld skydda sin integritet. För att tillgodose fundamentalisternas behov kan inte integritetsdesignmönstret överhuvudtaget tumma på integriteten.

Pragmatikerna (2) vill gärna använda sig av integritetsfrämjande verktyg och tjänster, men upplever att fördelarna som de konventionella tjänsterna erbjuder väger tyngre. För att pragmatikernas behov ska tillgodoses måste integritetsdesignmönstret ha integritet i beaktning, samtidigt som funktionaliteten och användarvänligheten är likvärdig de konventionella tjänsterna som finns på marknaden idag.

De Obekymrade (3) bryr sig inte att deras personliga information sparas och används på nätet, eller så är de helt enkelt omedvetna om att detta sker och kan således inte ta ställning till det. Eftersom denna grupp är obekymrade över integritet kan man tycka att de inte behöver tas i hänsyn, men som vi har diskuterat ovan är dagens användardatainsamling oetiskt och därför behöver denna grupp också inkluderas i vårt integritetsdesignmönsterförslag. För att denna grupp ska bli nöjda behöver integritetsdesignmönstret vara utformat på sådant vis att de inte upplever några försämringar jämfört med hur det var innan.

Dagens online-annonsering, där användares data samlas in, bearbetas och sammanförs för att erbjuda anpassat innehåll och riktad reklam, är oförsvarbar ur ett etiskt perspektiv. Utifrån

Jeroen van den Hovens (2008) grundprinciper kring integritetsetik så bidrar dagens online-annonsering till informationsbaserad skada, informationsbaserad ojämställdhet, informationsbaserad orättvisa samt moralisk autonomi och identifikation.

Problematiken här är att finansieringen bakom en stor del av internets innehåll kränker användares integritet, samtidigt som den möjliggör individanpassade annonser och tillgång till gratis innehåll. Internet är fyllt med "gratis" innehåll, vilket naturligtvis användare måste betala ett pris för. Priset är att utsättas för annonser. Men den ökande användningen av annonsblockerare tyder på att konsumenter är trötta på att bombarderas med påträngande reklam på nätet.

Annonsblockerare har i flera år erbjudit en enkel lösning för att slippa annonser, men detta har resulterat i att skada företag som betalar dyrt för annonser som ingen ser, vilket i längden även skadar utgivare eftersom incitamentet för annonsörer att köpa annonsplatser minskar. Annonsblockering kostar miljarder i förlorade intäkter vilket har lett till ett krig mellan utgivare och annonsblockerare där de försöker utmanövrera varandra. Utgivare och annonsörer har försökt att använda alternativa modeller såsom sponsrat innehåll, men dessa har inte fått någon positiv respons. Många webbplatser nekar tillgång för personer som använder annonsblockerare, men även denna åtgärd har inte varit lyckad.

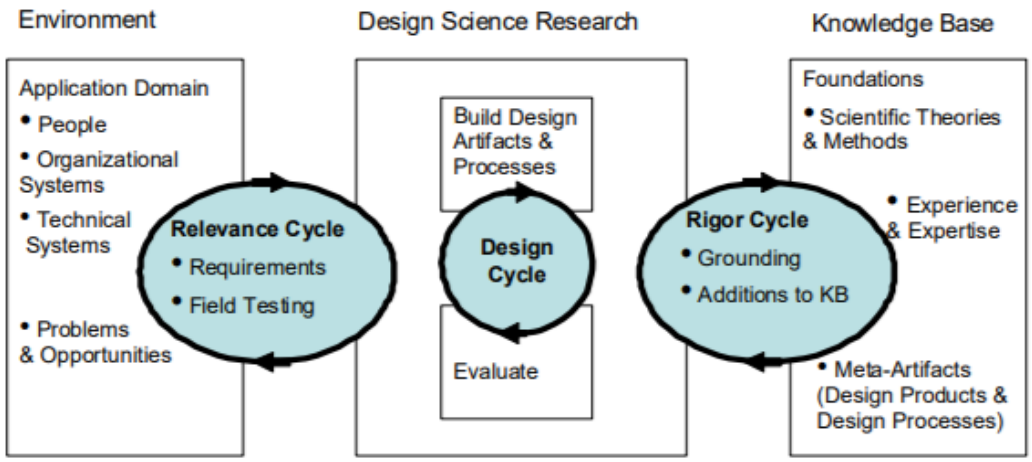
Många webbplatser är helt beroende av reklamintäkter, och när fler och fler använder annonsblockerare kan resultatet bli att användare får sämre eller inget innehåll alls och rätten till ett ”gratis internet” står på spel. Vi ser detta som en ohållbar situation som måste adresseras på något vis. Som det ser ut i nuläget är det en omöjlig ekvation: Användare vill inte se massvis med annonser, annonsörer vill inte betala annonser som ingen ser, utgivare behöver annonsörer för att kunna erbjuda gratis innehåll medan användare inte vill betala för innehåll.

Decentraliserad annonsering är en möjlighet för online-annonsering eftersom annonserna som distribueras till användaren sker på ett decentraliserat vis, t.ex. i webbläsaren. Genom att använda att decentraliserad annonsering kan användarens integritet skyddas eftersom både annonsörerna och utgivaren inte har tillgång till användardata, samtidigt som annonsörer fortfarande kan nå ut till kunder via en utgivare som får betalt för att tillhandahålla annonserna.

3 Metod

3.1 Metodval

Vi har val att använda oss av en kvalitativ metod, genom att intervjua experter inom de relevanta ämnena så kan vi få en djupare inblick i hur designmönstret bör förändras. Vår forskningsfråga utsätter att vi ska utvärdera ett integritetsdesignmönster som vi har skapat och inom *Design Science* så finns det många metoder som behandlar hur man ska gå till väga. Hevner är en av de mest framförhållna forskarna då han har skapat många metoder för hur man ska designa. Vi använder oss av hans *Three Cycle View* som en metod i vår process (Hevner, 2007). Metoden (se figur 2) är indelad i tre områden som måste behandlas i designprocessen. *Design Science Research* är kärnan i designmetoden, men när mönstret designas och utvärderas så används *Knowledge base* (litteraturen som vi behandlar i bakgrundskapitlet), och *Environment* (de existerande system som vi baserar mycket av vår design på).



Figur 2. Design Science Research Cycles (Hevner et al., 2004)

Enviroment och *Knowledge Base* existerar som ett stöd till designprocessen för att kontrollera att designen är relevant med vad litteraturen om ämnet behandlar och hur designen fungerar i omvärlden. Inom designcykeln så används en mer detaljerad process som har lagts fram av många olika forskare (Hevner et al., 2004; Peffers et al., 2007). Vi har använt Hevners sju riktlinjer i utformning av en design, vi har val att fokusera på de tre första punkterna eftersom de behandlar skapande och utvärdering av en design. I tabellen nedanför så visas vad varje punkt innebär, där störst fokus har hamnat på den tredje punkten *Design evaluation* eftersom den svarar på forskningsfrågan.

Design as an artifact:	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Problem relevance:	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Design evaluation:	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.

Tabell 1. Guidelines for design-science (Hevner et al., 2004).

En artikel som beskriver hur *Design science* artiklar bör utformas, visar hur ett forskningsbidrag ser ut inom *Design science* (Gregor & Hevner, 2013). Som figuren nedanför visar så finns det tre nivåer av mognad i en design. Vi har tagit en instans av en design och har utifrån den skapat ett mönster, vad vi egentligen har gjort är att göra designen mer mogen och har gått från nivå 1 till nivå 2. För att få detta att fungera så behövde vi använda oss av ett fungerande ramverk (nivå 3) som kan användas för att göra instansen mer abstrakt. Vi använde oss av *Privacy Patterns* vilket är ett ramverk för integritetsvänliga designer. Detta användes för att göra övergången från en instans (nivå 1) till ett mönster (nivå 2) möjlig.

Design Science Research contribution types	
Framework	Level 3
Pattern, Tool or Method	Level 2
Instance of design	Level 1

Tabell 2. Design Science Research contribution types (Gregor & Hevner, 2013)

Användningen av *Privacy Patterns* struktur har skapat en artefakt vilket är den första punken i Hevners riktlinjer (se Tabell 1). Mönstret består av sex olika rubriker: *Summary, Context, Problem, Solution, Consequences och Example.* Dessa rubriker skapar tillsammans en övergripande bild över problemen, dess lösning samt konsekvenserna som lösningen ger, men även exempel som gör det lättare för utvecklare att applicera ett mönster i deras system.

När mönstret var skapat så gick vi till nästa del av designprocessen. För att utvärdera mönstret används några olika arbetssätt som *Analysis* och *Descriptive* (Hevner et al., 2004). Vi har använt oss av experter inom ämnet för att få en bra analys och utformat frågorna så de förhåller sig till Hevners utvärderingsmetoder. Utöver intervjuerna så argumenteras och utvärderas också mönstret med hjälp av den *Knowledge Base* som vi presenterar i bakrundskapitlet. Genom intervjuerna och litteraturen utvärderas mönstret och ändras på de sätten som behövs tills vi kommer fram till en slutgiltig version.

Analysis	Analysis: Examine structure of artifact for static qualities (e.g., complexity) Architecture Analysis: Study fit of artifact into technical IS architecture Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance
Descriptive	Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility

Tabell 3. Improvement routine design (Hevner et al., 2004)

3.2 Datainsamling

En del av designutvärderingen är *Descriptive* som säger att man ska utvärdera genom att ha välunderbyggda argument som bygger på relevant forskning. Om ett giltigt argument kan ges till varför man har utformat delar av mönstret på ett visst sätt, kan det sedan användas för att säkerställa mönstrets värde. Datainsamlingen består av vad som diskuteras inom forskningen i de relevanta ämnena, från problemen till lösningarna.

3.2.1 Litteraturinsamling

För att hitta teori använde vi oss utav Google Scholar, LUBsearch för vetenskapliga artiklar samt har tjänster hemsidor där de förklara tjänstens funktioner. För att hitta relevant litteratur så har nyckelord som *Privacy, Privacy segmentation, Privacy by design, Privacy Patterns, digital advertising* och *decentralized advertising* används i sökningen. Litteraturen kan delas upp i tre stora huvudkategorier *Integritet*, *Design Patterns* och *Annonsering*. Dessa är det ämnena som är relevanta för denna uppsats, inom varje ämne så presenteras den teori som är relevant.

Integritet	Digital integritet Integritetsetik Integritetssegmentering
Designmönster	Privacy by design Privacy patterns
Annonsering	Digital annonsering Ad block Decentraliserad annonsering

Tabell 4. Genomgång av Tiddigre litteratur

3.3 Intervju

För att utföra analysdelen av Hevners utvärderingsprocess så har intervjuer utförts. Dessa har målet att få en mer analytisk utvärdering och därför har vi använt oss av experter inom integritet och designmönster för att få en djupare analys. Frågorna är utformade på ett sätt så att de kan ge så mycket värde som möjligt i vår utvärderingsprocess och följer därav Hevners riktlinjer.

3.3.1 Intervjuguide

Den design som har lagts fram måste utvärderas genom att låta experter analysera mönstret ur ett användbarhets-, kvalitets- och effektivitetsperspektiv (Hevner et al., 2004). Frågorna var utformade för att kunna låta intervjupersonerna att lättare ge kritik på vårt *Reward Attention* mönster. Man kan dela upp frågorna i tre olika delar som förhåller sig till de perspektiv som måste tas:

Behov och värde	• Finns det ett värde? • Behövs detta designmönster? • Hur tror ni användare kan dra nytta av detta design-mönster?
Tydlighet och förståelse	• Kan man förstå detta koncept tillräckligt för att imple-mentera/designa? Om inte vilken ytterligare information behövs i så fall ur ett utvecklingsperspektiv? • Håller sig designmönstret till designstandarder?
Positiva och negativa re-aktioner	• Vad ser ni för möjliga problem med detta designmöns-ter? • Vad ser ni för fördelar med detta designmönster?

Tabell 5. Genomgång av Intervjufrågor

Genom att dela in frågorna i dessa tre områdena kan man få bättre förståelse om vad som behövs förbättras. För att se om det finns ett behov eller värde så ställs frågor som försöker behandla detta område. På andra punkten som har frågorna designats för att belysa om mönstret är tydligt och förståeligt. Även intervjumetoden har anpassats för att se om mönstret är tydligt och förståeligt, genom att använda oss av en mailintervju så förhindrar det intervjupersonen förlitar sig på oss för att förstå mönstret. Detta är en viktig punkt då om mönstret inte är tydlig och förståelig nog av sig själv så kan det ej användas.

Sista området av frågor vill försöka få intervjupersonen att ta upp de problem som det ser kan ske med ett sådant mönster. Potentiella problem är viktiga då de måste finnas i mönstret för att uppmärksamma läsaren att designa sitt system på ett sätt som förhindrar de potentiellt negativa konsekvenserna.

3.3.2 Urval

I vår studie så är intervjupersonernas roll att kunna ge utvärdering av ett designmönster. De personer som vi har valt att intervjua behövde ha en expertis inom någon aspekt av det ämne som mönsterförslaget behandlar. Personer som forskar inom informatik och specialiserar sig inom integritet men även *design science* är relevanta. Vi har valt att fokusera på att intervjua akademiker då deras analytiska förmåga är mycket värdefullt i utvärderingsprocessen. Vi kontaktade organisationen *Privacypatterns.org* och fick kontakt med personen som hade ansvar för *Privacy Patterns* projektet. Eftersom denna person ligger bakom *Privacy Patterns* blev deras utvärdering av mönstret mycket värdefullt. Utöver personer som gav ett designperspektiv så kontaktade vi forskare som hade fokus på integritet och informationssäkerhet för att ge ett annat perspektiv.

I början av urvalsprocessen var det från menat att mjukvaruutvecklare skulle kontaktas för att utvärdera mönstret. Dock när vi fick tillbaka svar från intervjupersonerna ansåg de inte sig ha förmågan till att utvärdera mönster. Detta fick oss att tänka om och söka intervjupersoner som hade erfarenhet inom design science och med mer akademiska meriter då de hade en större förståelse och förmåga att utvärdera mönstret.

Namn:	**Expertis och erfarenheter:**
Nick Doty	Ansvarig för att upprätthålla *www.privacypatterns.org* och doktorand vid UC Berkeley School of Information.
Miranda Kajtazi	Universitetslektor vid Lunds universitet inom informatik med fokus informationssäkerhet

Tabell 6. Sammanställning Intervjupersoner

3.4 Etiska aspekter, Validitet & reliabilitet

För att hålla etiska aspekter så har vi varit väldigt transparanta med våra intervjupersoner. Vi har följt en metod som har tre krav, alla parter har gett samtycke, inte justera deras ord och att inte kränka deras privatliv (Jacobsen, 2002). När vi kontaktade våra intervjupersoner var vi tydliga med att förklara vad vi har gjort och vad deras del i forskningen är och hur de kommer användas i uppsatsen. Eftersom deras kunskap är viktig för att bekräfta deras validitet i deras utvärdering så har den hänvisats genom deras akademiska titlar, erfarenheter och forskningsfält.

Vårt bidrag är ett alternativ till dagens online-annonsering och kan leda till effekter som vi inte känner till som kan påverka berörda parter. Till exempel Youtube som har ett stort behov av annonser då det är de som finansierar deras plattform. Användning av vårt mönster hade kunnat påverka inte bara plattformen men även plattformens kreatörer som försörjer sig med hjälp av annonser. Men vi anser att vårt bidrag är en mer etisk metod och den kan implementeras för många digitala plattformar.

Som nämns tidigare så har vi baserat våra frågor på Hevners (2004) metoder vilket leder till mer valida svar från våra intervjupersoner. Utöver att frågorna har utformats från Hevners metoder så är det viktigt att intervjupersonerna har den relevanta kunskapen för att ge konstruktiv feedback. För att säkerställa att intervjupersonerna har rätt kunskap så har vi kontaktat personer som fokuserar på designmönster och integritet. Detta är anledningen till att vi har valt att använda oss av forskare inom de relevanta ämnena eftersom de har kunskapen för att kunna ge en värdefull utvärdering.

För att förhindra vår påverkan på intervjupersonerna så har vi utfört intervjuarna vid email. Vi anser att detta ger bättre validitet då vi inte kan hamna i positioner där vi förklarar för mycket och därav påverkar utvärderingen. Som nämnts tidigare så har Jacobsens (2002) riktlinjer följts för att intervjuerna har utförts på ett rätt sätt och resultat från intervjuerna är reliabelt.

4 Reward Attention

*Mönstret består utav sju beskrivande delar. Delarna är **sammanfattning**, **kontext**, **problem**, **lösning**, **konsekvenser**, **exempel** och slutligen en beskrivning av **kända användningsområden** av mönstret (se bilaga 1).*

4.1 Sammanfattning & kontext

I sammanfattningsdelen beskriver vi i grova drag syftet med mönstret. Vårt mönster ämnar att ge slutanvändare av diverse produkter och tjänster mer kontroll över när och hur deras personliga data hanteras på internet. Vidare ämnar mönstret att belöna slutanvändares användning av produkter och tjänster där de utsätts för reklam och annonser av olika slag – denna belöning baseras på deras respektive individuella *view-rate* (se bilaga 1). Således är detta mönster applicerbart i kontexten vi angett, nämligen för tjänster där insamlandet och sparandet av användardata görs för att kunna rikta annonser till slutanvändare (se bilaga 1). Mönstret riktar sig därmed till plattformar som exempelvis webbläsare som ett tillägg och inte till individuella hemsidor. Att flertalet hemsidor skulle utveckla egna lösningsvarianter med detta mönster som grund hade förmodligen inte varit önskvärt utan snarare lett till vidare otydlighet.

4.2 Problem

Problemen vi såg med vanliga annonseringsstrategier var att de samlar in och sparar användardata från deras användare för att kunna rikta relevanta annonser till användarna (se bilaga 1). Det är inte givet att alla användare som påverkas är medvetna om att detta sker eller förstår det på ett adekvat plan och riskerar därmed bli utnyttjade. Vidare medför det en potentiell integritetskränkning som exempelvis ett dataintrång skulle ske. Ett potentiellt problem med att användare upplever det jobbigt eller missledande med reklam kan vara en ökad användning av annonsblockeringsprogramvara, vilket i sin tur kan leda till, förutsatt att användningen är utbredd, att tjänster som i huvudsak försörjer sig via annonser inte längre kan erbjuda sina tjänster gratis (se bilaga 1).

4.3 Lösningar

Potentiella lösningar på ovanstående problem hade varit att kompensera slutanvändare för annonserna de utsetts för när de besöker olika sidor och använder exempelvis söktjänster på internet. Utöver kompensationen så borde det också ges mer kontroll till användaren angående

hur många, hur ofta och vilka typer av annonser som de vill se. Sedan för att adressera de användare som hade kunnat acceptera lösningen som vi har presenterat, men som motsätter sig att deras data lagras på en extern plats och att den data kan kopplas till dem som individ. För att det ska fungera så måste det även till ett decentraliserat och anonymiserat system så att företag inte behöver spara användardata på deras servrar. Istället sparas användardata och individers *view-rate* på deras lokala enheter (se bilaga 1).

Det bör nämnas att eftersom detta är ett designmönsterförslag som är frivilligt för utvecklare att använda för att proaktivt hantera integritetsproblem så är det inte vår uppgift att föreslå vilken typ av kompensation som ska utdelas. Detta är av två skäl:

1. Vi vet inte vad som är ekonomiskt hållbart för respektive användare av metoden
2. Vi vet inte vad som hade accepterats av olika tjänsters användare som kompensation.

4.4 Konsekvenser

Konsekvenser som vi ser med detta mönster är att datahantering endast kommer att sparas på respektive slutanvändares lokala enheter och kommer därmed inte gå att koppla till specifika användare. Det leder till att företag måste tänka om kring hur de riktar annonser och använder data för att identifiera vilka användare som är kan vara intresserade av vilka annonser. Vidare är en annan konsekvens att ett decentraliserat annonseringssystem och decentraliserat användardatalagringssystem måste existera eller skapas för att mönstret ska kunna appliceras (se bilaga 1).

4.5 Exempel

Exempel på hur ett applicerat mönster hade fungerat rent praktiskt från både slutanvändarens och de som erhåller tjänstens perspektiv, hade kunnat se ut som så att användaren anger sina annonseringspreferenser utefter lösningen vi presenterat ovan. När tjänsten som avses sedan används så visas annonser baserat på angivna användarpreferenser och deras respektive *view-rate* loggas för varje annons som de tittar på. När tjänsten, eller företaget, sedan får betalt för annonsörerna, för att de ska få lov att publicera sina annonser, så får också användaren kompensation baserat på deras *view-rate* per tittade annonser (se bilaga 1).

4.6 Kända användningsområden

Kända användningsområden avser riktiga exempel som antingen använt sig av mönstret för att designa sin lösning eller som omedvetet passar in i vad mönstret rent abstrakt ämnar uppnå. *BAT* och webbläsaren *Brave* är kända användningsområden för detta mönster. *BAT* är en nyttopollett, och efterliknar på många sätt en kryptovaluta, för en ny *blockchain* baserad digital annonsering och tjänsteplattform. *Brave* är en integritetsbaserad webbläsare som blockerar annonser som standard. *BAT* används just nu bara på *Brave* webbläsaren. *Brave* använder sig av något som kallas för *Brave Ads* som låter användaren välja om de vill ta del och se annonser och blir kompenserade för deras tid och uppmärksamhet på varje annons.

Kompensationssystemet är helt anonymt, informationen kring vilka annonser som användaren har sett lämnar inte deras lokala apparat och delas inte med någon, inte ens *Brave* har tillgång. Protokoll och kod är *open source* och tillgänglig för granskning (se bilaga 1).

5 Empiri

I vår empiri kommer intervjuernas viktigaste delar presenteras, men konversationerna i sin helhet finns som bilagor. Vi presenterar den information som kommer att användas för att utvärdera och korrigera den första versionen av *Reward Attention*. Empirin är uppdelad i de tre delarna som frågorna var uppdelade i, d.v.s. *behov och värde*, *tydlighet och förståelse* samt *positiva och negativa reaktioner*.

Namn:	**Expertis och erfarenheter:**
Nick Doty	Ansvarig för att upprätthålla *www.privacypatterns.org* och doktorand vid UC Berkeley School of Information.
Miranda Kajtazi	Universitetslektor vid Lunds universitet inom informatik med fokus informationssäkerhet

Tabell 6. Sammanställning Intervjupersoner

Vår första intervjuperson är Nick Doty, doktorand vid UC Berkeley School of Information. Han är involverad i *Privacy Patterns* projektet och är ansvaring för den amerikanska delen av projektet. Andra intervjupersonen är Miranda Kajtazi, forskare på Lunds universitet med fokus på informations och systemsäkerhet.

5.1 Behov & värde

Här presenteras svaren som behandlar behovet och värdet av *Reward attention.* Svaret som vi fick av Nick Doty indikerade att det verkligen finns ett behov av *Reward Attention.*

> *Overall, I think this could be very helpful. The idea of user participation is often lauded as a privacy-promoting strategy, but it's one that's less often actually implemented, compared to notice, minimization or control efforts. Explicitly rewarding attention seems like a way to increase transparency, to promote fairness by making the trade-off more direct, and to give users control in a way that isn't just turning something off.* (se bilaga 3)

Vidare utvecklar han att användningen av uppmärksamhetsbaserade lösningar kan ge integritetsvänlighet i system. Dock menar han att det ofta inte implementeras i system, då de ofta är överskuggade av andra integritetsstrategier som notiser, minimering och kontroll. Behovet och värdet finns men i nuläget så har inte tillräckligt med fokus lagts och det har överskuggat av andra integritetsskyddande metoder.

Något som Doty dock nämner är att med mer uppmärksamhets baserade metoder så kan man främja ett mer transparant utbyte mellan användare och företag. Idag är det ofta inte helt klart vad användaren ger i utbytte mot att använda tjänster på internet gratis. Om istället användaren ger deras uppmärksamhet genom att kolla på annonser och de får en kompensation i utbyte så blir utbytet mer tydligt och på så vis främjar en mer transparant och rättvis internetanvändning.

När vi intervjuar Miranda Kajtazi så säger hon också att behovet av integritetsrelaterande forskning har ett stort värde. Hon förtydligar även de lösningarna som *Reward Attention* föreslår, har ett stort värde vilket tyder på att det finns ett behov. Kajtazi nämner att hotet av icke integritetsvänlig hantering av användardata för att utnyttja användare i form av annonser är relevant. Metoder för att göra annonseringen så effektiv som möjligt blir ett större hot och någon form av skydd mot detta menar Kajtazi kommer att ha ett värde och behov.

> *(...) It is of utter most importance to tackle privacy also from the proposed pattern point of view, which often is critical, because we know that there are tracking websites that know what advertisements we watch, how long we watch them, even learning on the way more details about us: what are our interests within that advertisement and how they could lure us into them.* (se bilaga 5)

Dock är hon inte säker om att kompensation till användarna är det bästa sättet att lösa detta problem på. Hon menar att från ett psykologiskt perspektiv så kan kompensation fungera i vissa sammanhang men inte alltid, och att det krävs mer tester av *Reward Attention* för att säkerställa dess faktiska effekt innan man kan dra några slutsatser kring om *Reward Attention* funkar och om det faktiskt kan bidra med ett riktigt värde.

> *Rewards are a tricky aspect to tackle whether it is valuable or not. From a psychological perspective, rewards do functions in certain contexts, but not always, thus testing whether rewards attention will have more benefits is crucial before making any conclusions.* (se bilaga 5)

Kajtazi tycker inte att mönstret bidrar med ett värde till användaren, då hon menar att genom att ge kompensation i utbyte mot användardata skulle det fortfarande inte lösa problemet att användarens integritet kränks. Därav så bidrar *Reward Attention* inte med någon skillnad för användaren eftersom de fortfarande skulle få deras integritet kränkt.

> *I still don't find this plausibly beneficial to the users, since the solution only refers to the users being rewarded for giving part of their privacy while being exploited by the advertisement.* (se bilaga 5)

5.2 Tydlighet & förståelse

I intervjun med Doty eftersöker han fler exempel där ett *Reward Attention*-mönster har implementerats. Doty menar att med hjälp av flera exempel kan man identifiera de viktigaste delarna av ett mönster. Genom att hitta fler exempel på *Reward Attention* kan man lättare hjälpa framtida designers att se olika avvägningar från att implementera det på varierande sätt. I nuläget blir vårt exempel med Brave Browser och BAT mer av en integritetsanalys av en viss programvaruimplementering.

> *I'm not sure what the essential parts of the pattern are, as opposed to a particular solution. (...) identify some more examples of implementations in the wild — then you can pull out what parts do they all have in common and you can even help the future designers by seeing the trade-offs from implementing it one way or another. (...) Can you find another example that also implements the pattern but does it in a different way? That would really help in identifying the key parts of a pattern, rather than just doing a privacy analysis of a particular software implementation from Brave.* (se bilaga 3 & 4)

Doty menar vidare att mönstret hade gynnats av en snävare omfattning. Han tycker inte att decentraliserade annonser eller användarkontroll över annonser är nödvändiga för att belöna uppmärksamhet, utan ser de mer som separata mönster. Mönstret behöver tydligare differentiera belöning av uppmärksamhet och de mindre essentiella delarna eftersom decentralisering inte är nödvändigt för att åstadkomma kompensation till användare för att visade annonser. Slutligen tycker Doty att vi ska beskriva lösningen mer genomgående.

> *I'm not sure how much decentralized payment, or user controls over ads and their types, are important to rewarding attention or if those are just separate factors. (...) I'm also not clear on whether this is one pattern or two (or three). Is paying users for viewing ads the same as letting them choose topics and types of ads? Is decentralization necessary to accomplish this or can you reward attention through other means too?* (se bilaga 3 & 4)

Kajtazi tycker att vårt integritetsdesignmönsterförslag redovisar att kompensation av uppmärksamhet är ett bättre alternativ än dagens online-annonsering. Vi tolkar detta som att hon förstår mönstrets problemformulering och argumentation.

> *Yes, the description is reasonable to capture that the concept of reward attention is a better choice than the online form advertisements that is currently available on free services. (se bilaga 5)*

5.3 Positiva & negativa reaktioner

Doty beskriver att det finns vissa problem när det kommer till vårt första integritetsdesignmönsterförslag. Det första problemet han ser med vårt förslag är att vår problemformulering innehåller många antaganden. Han menar t.ex. att alla utgivare inte behöver spårning av användare för att kunna visa relevant reklam. Han köper heller inte riktigt vårt argument kring annonsblockeringsproblematiken i dagens online-annonsering, och tycker att vi bör undvika den i vårt integritetsdesignmönster.

> *Not all publishers need intensive tracking of users in order to show relevant advertising. I'm not sure the speculation about ad block implications is necessarily helpful either* (se bilaga 4)

Ett annat problem Doty ser med vårt integritetsdesignmönsterförslag, som är mer riktat mot integritetsdesignmönstrets egenskaper och mindre mot vår utformning, är potentiellt missbruk och illvillig användning av mönstret. Han menar att om uppmärksamheten måste specifikt identifieras för att kunna ge belöningar, uppkommer också risken att användarnas

uppmärksamhet övervakas. Vidare ser han även en möjlig problematik med att mönstret kan användas för att straffa eller utdra pengar från ouppmärksamhet av annonser.

> *Does attention have to be specifically identified in order to provide rewards for it? If so, what would the impact be on users if their attention is being monitored? Could it be used to punish or extract money from inattention.* (se bilaga 3)

Kajtazi ser inte att mönstret ändrar särskilt mycket utifrån ett integritetsperspektiv, utan anser snarare att det framförallt är ett fördelaktigt sätt för företag att locka användare till sina produkter. Hon tycker fortfarande att individens integritet är sårbar och tror mer på GDPR-liknade lösningar.

> *From a privacy perspective, the users are still vulnerable and not much changes with this new pattern. I would rather seek to bring to the user's attention more of a GDPR agenda. (...) From an organization's point of view, it might be beneficial for them to lure users into their products, but from the individual's privacy point of view there are no real benefits. (se bilga 5)*

Doty tycker att vårt integritetsdesignmönsterförslag kan vara till stor hjälp, och ville gärna titta på uppföljningar. Han tyckte särskilt att exemplet med BAT var bra och användbart. Hans förhoppning är att framöver kunna ta med detta integritetsdesignmönster i privacypatterns.org och därmed kunna få ännu mer feedback och utveckling.

> *Overall, I think this could be very helpful. (...) I'm happy to look at follow-ups. At some point I'd love to include this in the repository and get more feedback / development of it.* (se bilaga 3)

Även Kajtazi tycker att vårt integritetsdesignmönsterförslag skulle kunna vara till nytta för personlig integritet på nätet. Hon tror det är rimligt att anta att ett sådant mönster skulle kunna ändra på hur vi ser på individens integritet, särskilt när det kommer till gratistjänster.

> *(...) it sounds practically reasonable to assume that individual privacy might be looked differently if one knows that they could be rewarded to watch advertisement as opposed to being forced into is, particularly form the free service point of view. (se bilaga 5)*

6 Diskussion

I följande kapitel avser vi att bemöta hur innehållet i bakgrunden styrker vårt integritetsdesignmönsterförslag, samt redogöra vår empiri och hur den format vårt slutgiltiga integritetsdesignmönsterförslag.

6.1 Motiveringen till Reward Attention v1

6.1.1 *Etiskt* perspektiv

Reward Attention är ett integritetsdesignmönster som är designat i syfte att skapa en mer integritetsvänlig annonseringsmodell. Det finns många anledningar till att det finns ett behov av detta mönster. Inte minst ur ett etiskt perspektiv då skyddande av en användares integritet är en etiskt underliggande rättighet. Flertalet annonseringsmodeller som är i bruk idag kränker användares integritet eller gör inte tillräckligt för att ge användarna bättre integritet.

Genom att ta bort användares autonomi över deras användardata så kränker man deras integritet. Detta är ett av de problemen som *Reward Attention* (se bilaga 1) har i syfte att lösa genom att ge användare mer val och kontroll över hur deras data behandlas så får de mer autonomi över hur deras användardata behandlas. Vårt mönster är inte ensamma om att försöka att tillfredsställa denna punkt, GDPR har också försökt ge mer autonomi över användarens data. *Reward Attention* kan fungera som ett komplement till GDPR eftersom de tillfredsställer samma krav om autonomi.

Att användardata har ett stort värde är väldigt tydligt och framförallt för tjänsterna som använder det för att effektivisera annonseringsmetoder. Den data som tjänsterna samlar in om deras användare har en direkt påverkan på hur mycket det kan tjäna på deras annonser. Hur detta är ett problem ur ett etiskt perspektiv är att många tjänster inte tydliggör hur stort värdet av användardata är och när användarna inte medvetna av detta värde så finns det en risk att de ger bort mer i värde gentemot vad de får tillbaka i form av en given tjänst. *Reward Attention* (se bilaga 1) försöker lösa detta genom att både kompensera användaren för att den har gett användardata till tjänsten för att förtydliga att värdet av användarens data är stort och kräver en kompensation. Utöver det så vill mönstret ge mer kontroll till användaren vilket ger användaren alternativet att inte ge ut sin data till tjänster om de upplever att tjänstens värde inte är likställt med användarens data.

6.1.2 Integritetsegmentering

Integritetsdesignmönstret *Reward Attention* (se bilaga 1) tror vi kan lösa problemet med Westins integritetssegmentering genom att tillfredsställa alla tre gruppers integritetspreferenser. Fundamentalisterna erbjuds en integritetsfrämjande tjänst, pragmatikerna behöver inte väga integritet mot funktionalitet och de obekymrade kommer förhoppningsvis inte uppleva några försämringar jämfört med hur det var innan, utan kommer rimligen tycka det är bättre på grund av belöningen som tillkommer för sedda annonser.

Vår förhoppning är att integritetsdesignmönstret *Reward Attention* (se bilaga 1) kan erbjuda en lösning till problematiken vi ser finns kring dagens online-annonsering. Eftersom integritetsdesignmönstret låter användare få mer kontroll över deras data, samtidigt som den belönar

användares uppmärksamhet på annonser, uppfylls de etiska grundprinciper som finns kring integritet. Med decentraliserad annonsering kan online-annonsering bevaras och förbättras utan att missbruka användarens integritet. Marknadsförare kan fortfarande rikta relevanta annonser mot rätt målgrupp, mot specifika erbjudanden, samtidigt som konsumenter slipper att titta på annonser som inte intresserar dem. Annonsörer slipper betala dyra annonser som ingen tittar på, samtidigt som utgivare alltjämt kan erbjuda gratis innehåll till deras användare. Detta kan i längden innebära striden mellan annonsblockerare och utgivare, som kan komma att riskera det ”fria” Internet vi är vana vid idag, eventuellt kan undvikas.

6.1.3 Privacy by design & privacy patterns

Rådande eller potentiella integritetsproblem ska enligt *Privacy by design* lösas proaktivt och inte reaktivt. Den reaktiva lösningen för användarna och företagen är att på användarnas sida använda annonsblockerare av något slag och på företagens sida att förbjuda tillgång till innehåll om inte annonserna når fram. Den proaktiva lösningen för det problemet som vi har identifierat är att tänka om när det kommer till digital annonsering. Informera inte bara användarna att deras information används och hur den används, utan ge även användarna mer kontroll över hur och när deras information ska användas. Se inte den erbjudna tjänsten som kompensation till dina användare, utan ge dem något mer handgripligt i form av kompensation för att deras information används av företaget för att kunna rikta och locka till sig annonsörer. För att lyckas med detta så måste det tänkas om redan i designen av tjänster, produkter och det är här *Privacy Patterns* kan spela en stor roll. *Privacy Patterns* standardiserar utvecklingslösningar på integritetsproblem. För att hindra kapprustningen och vidare utveckling av reaktiva lösningar från vardera sida av den metaforiska skyttegraven, så har vi presenterat ett integritetsdesignmönster för att istället vara den proaktiva lösningen på problematiken kring digital annonsering och, från en stor del användare, den upplevda utnyttjningen som sker.

6.1.4 BAT

Mycket av byggstenarna till vårt mönster är baserat på ett redan existerande system som har en alternativ annonseringsmodell. *BAT* är ett alternativ till annonsering som har målet att skydda användarens integritet. Det fanns många delar av *BAT* som vi ansåg vara bra ur ett integritetsperspektiv och genom analysera hur de har löst dessa problem så kunde vi appliceras det i ett mönster. Målet med mönster är att förenkla hur *BAT* fungerar för att skapa ett mer effektiv och modulärt så det kan användas till fler sökmotorer som det används idag men även kunna applicera till andra delar på internet.

Sättet som *BAT* har valt att utföra deras annonsering och hur de förhåller sig till integritet är något som är ovanligt och nytt på marknaden. *BAT* är en stor del av *Brave* vilket är webbläsaren som använder sig av *BAT*. Om man ser till webbläsare marknaden så är de stora spelarna *Chrome*, *Safari* och *Firefox* men ingen av dem har en liknade affärsmodell för hur de ska hantera sina intäkter. Det har alla samma typ av modell vilket kan leda till ett kränkande till användares integritet. Även om *Firefox* marknadsför sig som en säkrare och mer integritetsvänlig sökmotor så är de ingen som har försökt att ändra hela affärsmodellen för att öka integritet. Därav så ser vi ett värde i att identifiera hur *Brave/BAT* fungerar och hur det har löst de integritetsproblem som uppstår i daglig användning på internet.

6.2 Utvärdering av Reward Attention

6.2.1 Värde & behov

En viktig punkt att utvärdera är om detta mönster verkligen har ett värde och om det som vi har skapat faktiskt kan användas. Både Doty och Kajtazi säger att integritet generellt och på det sättet som *Reward Attention* försöker lösa det, har en plats i dagens forskning kring integritet (se bilaga 3 & 5). Doty förtydligade att värdet och behovet i mönstret ligger i att den ökar transparensen mellan tjänster och användare. Men just nu så överskuggas detta sätt att bemöta integritet på tjänster med andra mer populära metoder. Med båda intervjuerna tillsammans med litteraturen så har vi konstaterat att värdet faktiskt finns och det är något som bör vidareutvecklas.

Dock så fick vi kritik över värdet på vissa delar av mönstret från Kajtazi då hon påpekar att mönstret inte ger något större värde till användarna (se bilaga 5). För version två av *Reward Attention* så har vi fokuserat på att vara tydliga med att mönstret ger en ökad transparens och kontroll vilket både följer punkter i *Privacy by Design* och det Doty nämner (se bilaga 3).

6.2.2 Sammanfattning

Ingen direkt kritik har lagts på just sammanfattningen, men detta är nog på grund av att sammanfattningen består av resten av mönstret. Då vi fått har konstruktiv kritik på resten av mönstret så per automatik så förändras sammanfattningen. Dock så behålls den korta längd och stora fokus på de viktiga delarna som problemet och lösningen. Eftersom sammanfattningens syfte är att ge en snabb helhetsbild så är det viktigt att vi fångar vad mönstret är och vilka problem det löser.

6.2.3 Kontext

Utifrån det Doty sa angående problemen så gjorde vi för många antagande och han nämnde att:

> *” Not all publishers need intensive tracking of users in order to show relevant advertising”* (se bilaga 4)

Även om han sa detta i sammanhang med problem-delen så är det fortfarande relevant i kontext-delen då vi har gjort samma antagande att detta mönster är applicerbart till tjänster som sparar och samlar data om deras användare. Därav så fick vi ändra vår kontext och minska våra påstådda antagande. Detta gjorde vi genom att ta bort antagandena helt och hållet och bara fokusera på kontexten att mönstret är applicerbart för tjänster som använder annonsering.

6.2.4 Problem

Vår första version av *Reward Attention* (se bilaga 1) led av att vi gjorde för många antagande gällande hur ”normal” annonsering sker. För att behandla det så har vi fokuserat mindre på hur annonsering fungerar och mer på universella problem. Som Doty (se bilaga 4) nämnde så finns det tjänster som inte behöver utnyttja användardata för annonsering. Därav så måste mer fokus läggas på vilka konsekvenser som sker, men framför allt att vi fokuserar på problemen som kärnan i *Reward Attention* löser. Mönstret är väldigt abstrakt och de kan lösa många olika problem beroende på hur man implementerar det. Till exempel om man vill lösa problemet men samtidigt vill ha ett större fokus anonymitet för användaren så kan ett decentraliserat system hjälpa, men man måste inte ha det för att implementera *Reward Attention*

Det som *Reward Attention* i grunden löser är att den förtydligar vad som användare ger i utbytte för att kunna använda sig av tjänster, särskilt när tjänsten är gratis. En tjänst som är transparant skapar förtroende hos användarna då det blir tydligare vad deras roll i tjänsten är. Utöver att transparens och utbytet blir tydligare så är också brist på kontroll av användarna ett problem som mönstret kan lösa.

6.2.5 Lösning

Första versionen av *Reward Attention* (se bilaga 1) omfattade flera lösningar i ett och samma mönster då vi även inkluderade användning av ett decentraliserat system för visning av annonser. I vår intervju med Doty framgick det att vårt mönsterförslag var något otydligt och att vi endast borde fokusera på just delen om kompensation för uppmärksamhet. Utifrån Dotys kritik tog vi bort allt annat som inte rörde kompensation för tittade annonser. Resultatet blev att *Reward Attention v2* (se bilaga 2) nu endast innefattar att användare kompenseras för deras annonstittande, och på så vis bidrar till att utbytet mellan användare och tjänsten tydligare och relationen mer transparent.

Vår förhoppning är att lösningen nu blir tydligare och lättare att förstå än föregående version. Vi ansåg detta var en viktig del att adressera eftersom det togs upp som kritik av Doty. Dock ifrågasatte Kajtazi om kompensation verkligen är en bra lösning på detta problem (se bilaga 5). Hon såg ett problem om kompensationer i sig verkligen har en positiv effekt men även att kompensation inte löser problemet att användaren får sin integritet kränkt då man fortfarande ger ifrån sig användardata. Dock så anser vi utifrån vad Doty sa (se bilaga 3) att eftersom användare nu informeras kring deras användardata och ge dem större kontroll värnas deras integritet på ett bättre sätt.

6.2.6 Konsekvenser

Likt lösning-delen tog vi bort allt som inte ingick i att kompensera användares uppmärksamhet och annonstittande. Konsekvenserna av mönstret i *Reward Attention v2* (se bilaga 2) blir istället att kompensation för uppmärksamhet ökar transparensen genom att tydliggöra vad respektive användare faktiskt byter mot att få använda sidan, samt att skapa mer rättvisa genom att göra utbytet mer direkt i form av kompensation till användare.

Kajtazi framförde kritik som menar att mönstret inte ändrar särskilts mycket och att individen fortfarande är sårbar. I skapandet av *Reward Attention v2* (se bilaga 2) hade vi en lite annorlunda syn på vad mönstret faktiskt ska uppnå, där vi nu mer ser det som ett sätt för användare att få mer transparens och en tydligare bild över vad som ges i utbytte mot användningen av en tjänst. I och med detta så bidrar inte mönstret med att de facto skydda användares integritet, utan är snarare ett verktyg som skapar klarhet och förbättrar den ojämställdhet som finns mellan användare och företag.

Vad som lades till i den nya versionen är att det finns en risk att kompensationen blir utnyttjad. I intervjun med Doty berör han risken med att ett sådant system skulle kunna övervaka användares uppmärksamhet och på så viss kunna skada eller utnyttja användare. Vi såg detta som ett utmärkt tillägg eftersom ett integritetsdesignmönster inte nödvändigtvis endast innebär positiva konsekvenser.

6.2.7 Exempel

Exempel-delen som vi använde i vår första version har vi inte fått någon specifik feedback på. Detta är förmodligen för att den var tillräckligt abstrakt och berörde endast användarkompensation och potentiell användarkontroll för att kunna även inkluderas i *Reward Attention v2* (se bilaga 2). Således förblir den oförändrad.

6.2.8 Kända användningsområden

Vårt första och enda kända användningsområde som vi använde i vår första version har behållits, då den exemplifierar en skarp användning av huvudkomponenterna av vårt mönster (se bilaga 1).

Det som har lagts till i vår andra version är ytterligare två användningsområden för mönstret (se bilaga 2). Detta gjordes då intervjupersonen Doty påpekade behovet och intresset för fler exempel där mönstret implementeras, men på olika sätt. Detta för att bättre kunna identifiera nyckelbitarna av mönstret, istället för att mönstret helt enkelt blir en integritetsanalys över en specifik mjukvaruimplementation från Brave (se bilaga 4).

7 Slutsats

Integritetsdesignmönstret som vi har skapat, och i denna uppsats utvärderat, ämnar bidra till ett mer integritetsvänligt sätt att hantera digital annonsering på internet. Syftet med *Reward Attention* är att öka transparensen mellan internettjänster och användare, genom att göra det mer tydligt vad utbytet mellan användaren och tjänsten är. Där användarna både ges kontroll över annonseringen dem utsätts för, men också kompenseras för deras annonstittande på en given tjänst eller produkt via ett givet medium – exempelvis via en sökmotor där annonstittandet avser betalda sökresultat.

Utöver det så lyfter mönstret tydligt upp en av kärnpunkterna i *Privacy by Design* vilket är transparens. Genom intervjuerna så har vi också konstaterat att det finns ett definitivt värde och behov för detta mönster. För att göra ”Reward Attention” mer användbart så har ramverket *Privacy Pattern* använts. Ett standardiserat ramverk ger mönstret ett större värde då den enklare kan kopplas ihop med andra *Privacy Patterns*.

Mötet mellan litteraturen och feedbacken från Nick och Miranda gjorde att vi kunde utveckla vårt mönster till något mer precist. Med feedbacken från Nick fick vi ett designperspektiv på vårt mönster. Därmed kunde vi bättre identifiera vad vårt mönster gör och bättre specificera vilka nyckelpunkter mönstret har. Vi ansåg initialt att vi hade ett tämligen snävt fokusområde, men fick ett nytt perspektiv från Nick. Vi blev varse om att vårt initiala mönster inte var tillräckligt abstrakt – utan det var snarare ett mönster baserat endast på ett exempel. Med feedbacken från Miranda fick vi ett mer användarcentrerat integritetsperspektiv och inte endast ett designerperspektiv. Detta gjorde att vi fick tänka ytterligare kring vilka effekter vårt mönster faktiskt har och inte har gentemot användaren.

Vid framtagandet av första versionen av *Reward Attention* lade vi stor vikt på att försöka tillgodose alla tre grupper som beskrivs i Westins integritetssegmenteringsteori. Inlägg som t.ex. decentraliserad annonsering fanns med så att integritetsfundamentalisterna även skulle vara nöjda. När *Reward Attention v2* blev allt mer komprimerad försvann många av de komponenter som gjorde att alla av Westins gruppers integritetsbehov blev tillgodosedda. Frågan är nu ifall Westins fundamentalister skulle acceptera eller se något värde med det nya mönstret. Vår intervju med Kajtazi indikerar att så inte är fallet, då det inte alls är säkert att kompensation och transparens räcker för dessa personer.

Vi har i nuläget adresserat de förbättringspunkter som vi har kunnat ta del av och de delar som vi själva identifierat, som visas i andra versionen av vårt mönster (se bilaga 2). Vi har dock som ambition att fortsätta utveckla och uppdatera vårt mönster. Vi har i samråd med Nick Doty pratat om en möjlighet att publicera vårt mönster på privacypatterns.org där den kan lagras och vidareutvecklas tillsammans med andra som medverkar till sidans innehåll. Således kommer mönstret att utvecklas av oss, men också av människor med helt andra erfarenheter och perspektiv. Vidare är det naturligt att mönstret inte blir helt och hållet färdigutvecklat, utan att det uppdateras i samband med den tekniska utvecklingen och tjänsterna där mönstret är applicerbart.

Bilaga 1

Bidrag till ett integritetsdesignmönster

Nedan följer vårt bidrag till katalogen av integritetsdesignmönster som vi anser fyller ett identifierat behov baserat på vårt litteraturkapitel. Vidare är denna bilaga första versionen av vårt integritetsdesignmönster.

Reward Attention

Sammanfattning

Detta mönster låter användare få mer kontroll över deras internet data och belönar deras uppmärksamhet på annonser baserat på deras respektive *view-rate.* Med en decentraliserad annonseringsprocess så kan digital annonsering bevaras och förbättras utan att missbruka användarens integritet.

Kontext

Detta mönster är applicerbart för tjänster som samlar och sparar användardata för annonsering.

Problem

Normala annonseringsstrategier utnyttjar deras användares integritet, genom att samla och spara användardata så kan relevanta annonser riktade till användare. Detta medför en potentiell integritetskränkning om ett dataintrång sker. Annonserna som användare utsätts för kan också uppfattas som jobbiga och i vissa fall missledande vilket leder till en ökad användning av ad-block mjukvaror. Detta riskerar att tjänster kan försörjer sig då annonser är en stor del av deras inkomster.

Lösning

Lösningen är att kompensera användaren för varje annons som det ser och ge dem val kring hur många, hur ofta och vilka typer av annonser som de vill se. Genom ett decentraliserat system så behöver företag inte spara användardata på deras servrar, användardata och *view-rate* sparas hos användaren lokala

Konsekvenser

Detta mönster låter individuella användares data att inte lämna deras lokala apparat men låter fortfarande användare att få relevanta annonser. Användardata kommer inte att kunna kopplas till en specifik användare då det bara sparas lokalt. En annan konsekvens är att en decentraliserad annonsering riktnings system och ett decentraliserat användardata lagrings-system.

Exempel

Användaren sätter deras egen annonserings preferenser. När man använder tjänsten så visas olika annonser och deras *view-rate* på varje annons loggas. När tjänsten får betalningen från annonsören så får också användaren en del baserad på *view-rate* per annons.

Kända användningsområden

BAT är en nyttopollett, efterliknar på många sätt en kryptovaluta, för en ny *blockchain* baserad digital annonsering och tjänsteplattform. Brave är en integritets baserad webbläsare som blockerar annonser som standard. BAT används just nu bara på Brave webbläsaren. Brave använder sig av något som kallas för Brave Ads som låter användaren välja om de vill ta del och se annonser och blir kompenserade för deras tid och uppmärksamhet på varje annons. Kompensationssystemet är helt anonymt, informationen kring vilka annonser som användaren har sett lämnar inte deras lokala apparat och delas inte med någon, inte ens Brave har tillgång. Protokoll och kod är *open source* och tillgänglig för granskning.

Bilaga 2

Andra versionen av vårt bidrag till ett integritetsdesignmönster

Nedan följer andra versionen av vårt bidrag till katalogen av integritetsdesignmönster som vi anser fyller ett identifierat behov baserat på vårt litteraturkapitel och baserat på mötet av vår litteratur och empirin vi samlat in.

Reward Attention v2

Sammanfattning

Detta mönster kompenserar användare för deras uppmärksamhet på exempelvis annonser när de använder tjänster som visar annonser och reklam för sina användare – detta för att tydliggöra vad som ges i utbyte mot att använda en given internettjänst. Mönstret ger också användaren mer kontroll på ett annat sätt än att bara slå av någonting fullständigt.

Kontext

Detta mönster är applicerbart för tjänster visar reklam och annonser till deras användare.

Problem

Internettjänster som kan erhållas av en användare i utbyte mot att de utsätts för reklam så råder det idag en otydlighet kring vad som användaren faktiskt ger i utbyte mot möjligheten att använda tjänsten som avses. Det är vanligt att användare vet vad dem får i och med användandet av tjänsten, men inte vad de ger i utbyte. Vidare finns det en brist på kontroll från användarnas sida i hur och när de kollar på eller utsätts för annonser.

Lösning

Lösningen är att kompensera användaren för annonser som de utsätts för när de använder olika tjänster. Om en sådan kompensation finns där användare belönas på något sätt för deras annonstittande så blir utbytet mellan användare och tjänsten tydligare och därav blir relationen mer transparent. Ett tillägg som hade gjort relationen ännu mer transparent hade varit att ge användarna mer kontroll över hur deras annonstittande ser ut och sker – detta kopplat med kompensationslösningen.

Konsekvenser

Genom att belöna användares uppmärksamhet så ökar transparensen genom att tydliggöra vad respektive användare faktiskt byter mot att få använda sidan, det främjar rättvisa genom att göra utbytet mer direkt i form av kompensation till användare. Vidare hade det gett användarna mer kontroll över deras annonstittande.

Exempel

Användaren sätter deras egen annonserings preferenser sett till hur ofta de vill se dem. När man använder tjänsten så visas olika annonser och deras *view-rate* på varje annons loggas. När tjänsten får betalningen från annonsören så får också användaren en del baserad på *view-rate* per annons.

Kända användningsområden

(1) *BAT* är en nyttopollett, efterliknar på många sätt en kryptovaluta, för en ny *blockchain* baserad digital annonsering och tjänsteplattform. *Brave* är en integritets baserad webbläsare som blockerar annonser som standard. *BAT* används just nu bara på *Brave* webbläsaren. *Brave* använder sig av något som kallas för *Brave Ads* som låter användaren välja om de vill ta del och se annonser och blir kompenserade för deras tid och uppmärksamhet på varje annons. Kompensationssystemet är helt anonymt, informationen kring vilka annonser som användaren har sett lämnar inte deras lokala apparat och delas inte med någon, inte ens *Brave* har tillgång. Protokoll och kod är *open source* och tillgänglig för granskning.

(2) *CookApps* är ett företag som skapar mobilapplikationer och använder sig av videoannonser i sina spel exempelvis för att ge deras användare ett extra liv om de kollar på en annons. De har valt att lägga den typen av annonser strategiskt där de tror att deras användare kommer behöva exempelvis det extra livet.

(3) *Reddit* är en social plattform där användare kan interagera med varandra via text i olika sektioner som i sin tur är inriktade på olika intresseområden. De finansierar sin sida främst genom annonser som deras användare ser när de använder deras hemsida. *Reddit* har lanserat ett test av deras egen kryptovaluta på två sektioner, eller *subreddits*, där användare kan tjäna kryptopolletterna exempelvis när de publicerar en kommentar, lägger upp en länk, startar en ny tråd osv. Kryptovalutan kan användas för att köpa exklusiva märken som kan användas på sajten, använda sig av animerade emojis och kan även användas till att svara på andra användare med *graphics interchange format* (GIFs). *Reddit* ger sig själva tjugo procent av kryptopolletterna som distribueras.

Bilaga 3

Mejlkonversation och svar på frågorna av Nick Doty:

SG = Studentgruppen

ND = Nick Doty

SG:

Hi Nick,

Hope you are well!

We are three students from Lund University, Sweden, writing our thesis paper for our bachelor's degree in system science. Our names are Linus Nilsson, Victor Lindstrand and Jonas Werne. The focus of our thesis paper is to evaluate a privacy pattern that we have made, based on the possible need for it and our design.

The title of our paper is:

Reward Attention: ***Proposal for a privacy design pattern***

We would be immensely grateful if you would like to evaluate our privacy pattern by reading it and answering seven questions regarding the pattern.

We of course understand that you are busy and especially with regards to the corona virus and the strain it has put on universities worldwide that you might not have time to aid us in our paper - but we would nonetheless be extremely grateful if you would consider it.

If you would be inclined to evaluate our privacy pattern and aid three students in their thesis paper, then we can send our design pattern to you by e-mail accompanied by our seven questions.

All the best,

Linus, Victor & Jonas

ND:

Hi Linus,

I hope you and yours are handling the public health crisis as well as can be expected.

I would be happy to read and respond to your work on privacy design patterns. My hope is that can be a collection of contributions from many people. Let me know what you're looking for, and when you would need feedback for your thesis timeline.

Sincerely,

Nick

SG:

Hi again Nick,

Thank you for responding to our email!

We have attached our privacy design pattern in this email.

We would be grateful for any feedback you would and could give us regarding anything about the pattern.

If you would like specific questions we have attached those as well in a separate document. Although we suspect you might be better equipped on your own to evaluate it.

Are we missing anything for this to be a completed pattern?

We have our final submission of our thesis paper on the 20th of May this year, so feedback before that date would be appreciated - even though we realize that this is within 18 days.

All the best.

Linus, Victor & Linus

ND:

Hi Linus and colleagues,

Thanks for sending this along, and for following up with me. It has been hard to focus and keep on a schedule at the moment. But I found it interesting to read over this pattern and questions this afternoon. I've attached an annotated PDF with some comments on particular sections of the pattern text.

Overall, I think this could be very helpful. The idea of user participation is often lauded as a privacy-promoting strategy, but it's one that's less often actually implemented, compared to notice, minimization or control efforts. Explicitly rewarding attention seems like a way to increase transparency, to promote fairness by making the trade-off more direct, and to give users control in a way that isn't just turning something off. There are a couple draft patterns in the repository now that might be relevant, but they're also not very fleshed out (Pay Back, Reciprocity, Incentivized Participation).

My main concern is that I'm not sure what the essential parts of the pattern are, as opposed to a particular solution. I think it would most help to identify some more examples of implementations in the wild — then you can pull out what parts do they all have in common and you can even help the future designers by seeing the trade-offs from implementing it one way or another. As it is, I'm not sure how much decentralized payment, or user controls over ads

and their types, are important to rewarding attention or if those are just separate factors. And I think a designer or developer would definitely benefit from more detailed advice on how to implement rewarding attention, including what has worked and what pitfalls or concerns to avoid.

Hope this helps and I look forward to seeing more. Congrats on making it through a bachelor thesis project!

Cheers,

Nick

Some comments inline on some of your particular questions:

• Can you understand this concept enough to be able to implement/design a solution? If not what further information is needed to be able to implement/design a solution?

• Is there a value for this type of privacy pattern?

• Is there a need for this type of privacy pattern?

• Does this privacy pattern adhere to design standards?

• How do you think users can benefit from this privacy pattern?

• What potential problems do you see with this privacy design pattern?

I think it would be worth thinking explicitly about ways the idea could be abused or users harmed. Does attention have to be specifically identified in order to provide rewards for it? If so, what would the impact be on users if their attention is being monitored? Could it be used to punish or extract money from inattention? (Isn't there a Black Mirror episode of that?) Better still would just be finding some more examples in the wild and seeing what problems really do arise.

• What potential benefits do you see with this privacy design pattern?

• Would you be willing to evaluate a possible follow-up version of this privacy design pattern after improvements has been made?

Sure, I'm happy to look at follow-ups. At some point I'd love to include this in the priva-cypatterns.org *repository and get more feedback / development of it*

Bilaga 4

Kommentarer från Nick Doty på *Reward Attention* Version 1:

Kommentarer från problemdelen:

A lot of assumptions here. Not all publishers need intensive tracking of users in order to show relevant advertising. I'm not sure the speculation about ad block implications is necessarily helpful either.

Kommentarer på Lösningsdelen:

Tell us more about this solution!

I'm also not clear on whether this is one pattern or two (or three). Is paying users for viewing ads the same as letting them choose topics and types of ads? Is decentralization necessary to accomplish this or can you reward attention through other means too?

Kommentarer på Kända andvändningsområden

This is a good and useful example.

Can you find another example that also implements the pattern but does it in a different way? That would really help in identifying the key parts of a pattern, rather than just doing a privacy analysis of a particular software implementation from Brave.

Bilaga 5

Svar på frågorna av Miranda Kajtazi:

Can you understand this concept enough to be able to implement/design a solution? If not what further information is needed to be able to implement/design a solution?

Yes, the description is reasonable to capture that the concept of reward attention is a better choice than the online form advertisements that is currently available on free services.

Is there a value for this type of privacy pattern?

Rewards are a tricky aspect to tackle whether it is valuable or not. From a psychological perspective, rewards do functions in certain contexts, but not always, thus testing whether rewards attention will have more benefits is crucial before making any conclusions.

Is there a need for this type of privacy pattern?

Privacy has dominated most of the talk in the last decade, following fresh new talks in the current one. It is of utter most importance to tackle privacy also from the proposed pattern point of view, which often is critical, because we know that there are tracking websites that know what advertisements we watch, how long we watch them, even learning on the way more details about us: what are our interests within that advertisement and how they could lure us into them.

Does this privacy pattern adhere to design standards?

I am not a design expert, but it sounds practically reasonable to assume that individual privacy might be looked differently if one knows that they could be rewarded to watch advertisement as opposed to being forced into is, particularly form the free service point of view.

How do you think users can benefit from this privacy pattern?

I still don't find this plausibly beneficial to the users, since the solution only refers to the users being rewarded for giving part of their privacy while being exploited by the advertisement.

What potential problems do you see with this privacy design pattern?

From a privacy perspective, the users are still vulnerable and not much changes with this new pattern. I would rather seek to bring to the user's attention more of a GDPR agenda.

What potential benefits do you see with this privacy design pattern?

From an organization's point of view, it might be beneficial for them to lure users into their products, but from the individual's privacy point of view there are no real benefits.

Would you be willing to evaluate a possible follow-up version of this privacy design pattern after improvements has been made?

Yes.

Bilaga 6

Mejlkonversation med Miranda Kajtazi om *Reward Attention* Version 1:

SG: Studentgruppen

MK: Miranda Kajtazi

SG:

Hi Miranda,

Hope you are well!

Victor and me (Linus) both took your *Information Security* course.

We are three students from Lund University, Sweden, writing our thesis paper for our bachelor's degree in system science. Our names are Linus Nilsson, Victor Lindstrand and Jonas Werne. The focus of our thesis paper is to evaluate a privacy pattern that we have made, based on the possible need for it and our design.

The title of our paper is:

Reward Attention: ***Proposal for a privacy design pattern***

We would be immensely grateful if you would like to evaluate our privacy pattern by reading it and answering seven questions regarding the pattern.

We of course understand that you are busy and especially with regards to the corona virus and the strain it has put on universities worldwide that you might not have time to aid us in our paper - but we would nonetheless be extremely grateful if you would consider it.

If you would be inclined to evaluate our privacy pattern and aid three students in their thesis paper, then we can send our design pattern to you by e-mail accompanied by our seven questions.

All the best,

Linus, Victor & Jonas

MK:

Sure, we can give it a try. I am not in design of secure systems, but you will list my expertise under scientific perspectives, so it should be different to have my views on it.

When do you plan for this?

SG:

Hi Miranda,

Since we are doing something more practical for our thesis paper, we have more curated questions that we would like answered. Both our privacy design pattern and the related questions are attached to this email. If you have any thoughts, questions or criticisms beyond our questions we would be more than happy to listen and abide.

Following is a short summation of what privacy design patterns are:

> *Privacy represents a broad variety of concerns — subjective, contextual, hard-to-define — that real people have about the flows of personal information.*
>
> *Translating these concerns (as well as corporate and legal liability) into technical artifacts — a process known generally as "privacy-by-design" — has proven difficult. How can we best convert lawyer speak into engineering speak? How can problems be elegantly anticipated early in the development process?*
>
> *Drawing inspiration from Christopher Alexander and the success of software design patterns in improving communication about tried-and-true practices, we hope privacy patterns will:*
>
> - *standardize language for privacy-preserving technologies*
> - *document common solutions to privacy problems*
> - *help designers identify and address privacy concerns*

You can evaluate our pattern at your convenience and at any time you see fit.

The final submission of our thesis paper is 20th May this year.

All the best,

Linus, Victor & Jonas

Referenser

Birnbaum, E. (2019). Google 'leaked' personal data to other companies, rival claims. Retrieved from https://thehill.com/policy/technology/459857-google-leaked-personal-data-to-other-companies-rival-claims

Colesky, M., Hoepman, J.H., Hillen, C. (2016). A critical analysis of privacy design strategies. *2016 IEEE Security and Privacy Workshops (SPW)*, 33-40.

Datainspektionen. En Introduktion till dataskyddsförordningen. Retrieved from https://www.datainspektionen.se/vagledningar/en-introduktion-till-dataskyddsforordningen/

Davies, S. (2010). Why Privacy by Design is the next crucial step for privacy protection.

Englehardt, S., Reisman, D., Eubank, C., Zimmerman, P., Mayer, J., Narayanan, A., Fel-ten, E.W. (2015). *Cookies that give you away: The surveillance implications of web tracking.* Paper presented at the Proceedings of the 24th International Conference on World Wide Web.

Evans, D. S. (2009). The Online Advertising Industry: Economics, Evolution, and Privacy. *Journal of Economic Perspectives, 23*(3), 37-60.

Google. (2020). View rate: Definition. Retrieved from https://support.google.com/google-ads/answer/6293479?hl=en

Gregor, S., Hevner, A.R. (2013). Positioning and presenting design science research for maximum impact. In *MIS quarterly* (pp. 337-355).

Griffin, A. (2017). Yahoo Hack: Company Leaked Details Of Every Single Person Who Uses It. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/yahoo-hack-details-personal-information-was-i-compromised-affected-leak-a7981671.html

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems, 19*(2), 4.

Hevner, A. R., March, S.T., Park, J., Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105.

Hill, K. (2012). How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Retrieved from https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#6a993c266668

Holvast, J. (1993). *Vulnerability and privacy: are we on the way to a risk- free society?* Paper presented at the IFIP-WG9.2 conference.

Hoofnagle, C. J., Urban, J.M. (2014). Alan Westin's privacy homo economicus. *Wake Forest L. Rev., 49*, 267.

IAB. (2016). Ad Blocking: Who Blocks Ads, Why and How to Win Them Back. *International Advertising Bureau*.

Iqbal, U., Shafiq, Z., Qian, Z. (2017). *The ad wars: retrospective measurement and analysis of anti-adblock filter lists.* Paper presented at the Proceedings of the 2017 Internet Measurement Conference.

Ivanjko, T., Bezjak, T. (2017). The Influence of Ad Blockers on the Online Advertising Industry. 291.

Jacobsen, D. I., Sandin, G. (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*: Studentlitteratur.

Krebs, B. (2013). Adobe Breach Impacted At Least 38 Million Users. Retrieved from https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/

Kumaraguru, P., Cranor, L.F. (2005). Privacy indexes: a survey of Westin's studies In (pp. 5): Carnegie Mellon University, School of Computer Science, Institute for Software Research International.

Lahtinen, M. (2019). *Allmänhetens uppfattning om användningen av bevakningskameror i samhället*. Retrieved from LUSAX-säkerhetsforskargrupp: https://www.lusax.ehl.lu.se

Mayer, J. R., Mitchell, J.C. (2012). *Third-party web tracking: Policy and technology.* Paper presented at the 2012 IEEE Symposium on Security and Privacy

Montero, J. P. (2000). Optimal design of a phase-in emissions trading program. *Journal of Public Economics, 75*(2), 273-291.

Moor, J. (1990). The ethics of privacy protection. *Library trends, 39*(1-2), 69-82.

Newman, N., DAL Levy, RK Nielsen. (2015). Reuters Institute Digital News Report 2015: Tracking the Future of News. *Reuters Institute for the Study of Journalism*.

Ordböcker, S. A. (2015). Integritet. Retrieved from https://svenska.se/saol/?id=1292471&pz=7

PageFair. (2015). The cost of ad blocking: 2015 Global Adblock report. *PageFair*.

PageFair. (2017). The state of the blocked Web: 2017 Global Adblock report. *PageFair*.

PageFair. (2020). Growth of the Blocked Web: 2020 Global Adblock report. *PageFair*.

Patterns, P. (2020). About. Retrieved from https://privacypatterns.org/about/

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.

Preibusch, S. (2014). *Managing diversity in privacy preferences: How to construct a privacy typology.* Paper presented at the Workshop on Privacy Personas and Segmentation, co-located at the 10th Symposium On Usable Privacy and Security (SOUPS).

Rosenberg, E. (2018). How Google Makes Money (GOOG). Retrieved from https://www.investopedia.com/articles/investing/020515/business-google.asp

Rosenberg, R. (1992). The social impact of computers. *Academic Press Inc.*

Ryan, J. (2019). Google faces first investigation by its European lead authority for “suspected infringement” of the GDPR, following formal complaint from Brave. Retrieved from https://brave.com/dpc-google/

Searls, D. (2015). How Will the Big Data Craze Play Out? *Linux Journal*.

Shewan, D. (2020). The Rise of Ad Blockers: Should Advertisers Be Panicking? Retrieved from https://www.wordstream.com/blog/ws/2015/10/02/ad-blockers

Shiller, B., Waldfogel, J., Ryan, J. (2017). Will Ad Blocking Break the Internet? *National Bureau of Economic Research, No. w23058*.

Software, B. (2018). Basic Attention Token (BAT) Blockchain Based Digital Advertising. Retrieved from https://basicattentiontoken.org/wp-content/uploads/2017/05/BasicAttentionTokenWhitePaper-4.pdf

Swinhoe, D. (2020). The 15 biggest data breaches of the 21st century. Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Tene, O., Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop., 11*, xxvii.

UK, I. (2019). Ad Blocking: Consumer Usage and Attitudes. *International Advertising Bureau UK*.

Urban, J. M., Hoofnagle, C.J. (2014). The privacy pragmatic as privacy vulnerable. *Symposium on Usable Privacy and Security (SOUPS 2014) Workshop on Privacy Personas and Segmentation (PPS)*, 1-2.

Van Den Hoven, J. (2008). Information technology, privacy, and the protection of personal data. *Information technology and moral philosophy*, 301-322.

Vance, J. (2008). Five data leak nightmares. Retrieved from https://www.networkworld.com/article/2289232/five-data-leak-nightmares.html

Williams, M. (2017). Inside the Russian hack of Yahoo: How they did it. Retrieved from https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html

WordStream. (2020). Click-Through Rate (CTR): Understanding Click-Through Rate for PPC. Retrieved from https://www.wordstream.com/click-through-rate