

Hva vet appen om deg?

Kartlegging av personvernutfordringer knyttet til mobilapplikasjoner

Atle Årnes og Catharina Nes
15. september 2011



Sammendrag

Mobilapplikasjoner, såkalte "apps", er et marked i kraftig vekst. Flere hundre tusen applikasjoner er tilgjengelig for nedlasting fra ulike "app-stores". Appene kan være morsomme, praktiske og enkle å bruke. Mange apper håndterer imidlertid også store mengder personopplysninger om sine brukere, ofte uten at brukeren selv er klar over dette.

Fra et brukerperspektiv er app-markedet preget av liten grad av gjennomsiktighet når det gjelder *hvilke* opplysninger som samles inn om brukeren, hva som er *formålet* med innsamlingen og hvordan opplysningene eventuelt *viderebrukes*.

Brukeren må ved nedlasting av appen ta stilling til om han tror at personopplysninger vil bli håndtert på en akseptabel måte. På grunn av mangelfull informasjon til brukeren må denne transaksjonen i stor grad baseres på tillitt til de ulike app-aktørene. Brukere av iPhone overlater håndteringsnivået for personopplysningene sine til Apple, som gjennom forhåndsgodkjenning av alle apper garanterer at disse oppfyller bestemte krav. Fra et brukerståsted kan man sammenligne iOS-plattformens håndtering av personopplysninger som å åpne en låvedør inn til telefonen. Når først låvedøren er åpnet vil brukeren ikke vite sikkert hvilke opplysninger som går igjennom den, men må velge å stole på at Apple har full kontroll over appene og hva disse kan hente ut.

Androids håndtering av personopplysninger kan illustreres som det å åpne veldig mange luker. Når lukene først er åpnet vil brukeren imidlertid ha liten kontroll med hva som går igjennom dem. Her er ingen annen autoritet som passer på. Brukeren kan la være å installere applikasjoner som ser ut til å åpne luker (åpne for informasjon) som brukeren ikke ønsker å gi applikasjonen tilgang til. En Android-bruker vil, sammenlignet med iPhone-brukeren, kunne foreta en litt mer kvalifisert vurdering av hver enkelt applikasjon før nedlasting. Likevel må Android-brukeren også basere installasjonen av appen på tillit.

App-markedet er preget av uklare ansvarsforhold og mange ulike aktører å forholde seg til. Sentrale aktører, foruten sluttbruker, er mobiltelefonleverandører, operativsystemleverandører, app-leverandører, app-utviklere, app-oppdragsgivere og diverse tredjeparter som analyseselskaper og markedsførere. Behandlingsansvaret for en applikasjon må plasseres i hvert enkelt tilfelle, på bakgrunn av formålet med innsamlingen av personopplysningene og kontraktsmessige forhold mellom partene. Den ansvarlige får blant annet en opplysningsplikt med hensyn til hvordan man håndterer personopplysninger.

Rettigheten til informasjon om, og innsyn i behandlingen av egne personopplysninger er viktige personvernprinsipper. Ingen av de norske applikasjonene Datatilsynet har sett på har lett tilgjengelig informasjon til brukeren om hvordan de håndterer personopplysningene som samles inn.

Muligheten til å legge ut informasjon om hvordan appen håndterer personopplysninger i App Store eller Android Market, benyttes sjelden. Dersom dette i større grad hadde blitt gjort ville brukeren før installasjonstidspunktet hatt et bedre grunnlag til å ta en kvalifisert beslutning om å installere appen eller ikke. Videre legges det sjelden inn informasjon i selve appen om hvordan den håndterer personopplysninger. Det er verdifullt å legge ut informasjon også her slik at brukeren har den lett tilgjengelig også etter at applikasjonen er lastet ned.

Endelig er det viktig at behandlingsansvarlig for en applikasjon også legger ut informasjon om hvordan appen håndterer personopplysninger på nettsiden som app-ansvarlig råder over. Denne muligheten benyttes sjelden, men er viktig for å gi informasjon til brukeren før installasjonstidspunktet, samt for å få klargjort ansvarsforhold (behandlingsansvar) og jurisdiksjon tydeligere.

Innhold

Sammendrag	2
1 Innledning.....	6
1.1 Problemstilling.....	6
1.2 Metode og ressurser	7
2 Kort om markedet for mobilapplikasjoner	8
2.1 Hva er en "app"?	8
2.2 Apple vs. Android	8
2.2.1 Apple - iOS	9
2.2.2 Android	10
2.3 Hvem skjuler seg bak en app?	11
2.3.1 Applikasjonsutvikler	11
2.3.2 App-bestiller	11
2.3.3 Tredjeparter.....	12
2.3.4 Operativsystemleverandører og app-leverandører	12
2.3.5 Mobiloperatørene	13
2.3.6 Mobiltelefonleverandørene	13
3 Hva vet appene om deg?.....	13
3.1 Hvilke opplysninger henter appene ut?	13
3.1.1 Lokasjonsdata	15
3.1.2 Identifiserende opplysninger	16
3.1.3 Kontaktopplysninger	16
3.1.4 Kalenderdata	17
3.1.5 Kamera og mikrofon.....	17
3.1.6 Gyroskop og akselerometer	17
4 Mangel på kontroll og oversikt.....	18
4.1 System basert på tillit.....	18
4.2 Fravær av informasjon	18
5 Uklare ansvarsforhold	20
5.1 Hvem er behandlingsansvarlig?	21
5.1.1 Forholdet mellom utvikler og oppdragsgiver	21
5.1.2 Forholdet til tredjeparter	22
6 Andre juridiske spørsmål.....	23
6.1 Avtale er utgangspunktet	23

6.2	Retten til innsyn og informasjon	23
6.3	Forholdet til annet lovverk	24
7	Konklusjon	25
8	VEDLEGG.....	26
	Vedlegg 1: Norske Android-apper gjennomgått i rapporten.	26
	Vedlegg 2: Utenlandske Android-applikasjoner gjennomgått i rapporten.....	27
	Vedlegg 3: Liste med spørsmål sendt til norske app-utviklere	28
	Vedlegg 4: Eksempel fra informasjonsside i Android Market	29
	Vedlegg 5: Oversikt over samtlige informasjonselement appene krever tilgang til	30
	Vedlegg 6: Gjennomgang av norske apper med personvernerklæring	31

1 Innledning

Mobilapplikasjoner, såkalte ”apps”, er et marked i kraftig vekst. Flere hundre tusen applikasjoner er tilgjengelig for nedlasting fra ulike ”app-stores”. Appene kan være morsomme, praktiske og enkle å bruke - med et fingertrykk kan man sjekke været, spille spill eller finne ut når bussen går. Mange apper håndterer imidlertid også store mengder personopplysninger om sine brukere, ofte uten at brukeren selv er klar over dette. Enkelte apper krever tilgang til personopplysninger som kan fortelle svært mye om deg, som for eksempel hvor du har oppholdt deg de siste dagene, hvem dine venner er og hvilke interesser du har.

En nylig gjennomført undersøkelse blant amerikanske smarttelefonbrukere fant at 38 % satte personvern som deres primære bekymring ved bruk av mobile apps¹. Nesten alle som ble spurt i undersøkelsen sa at de ønsket mer transparens ved behandling av personopplysninger og kontroll på hva opplysningene benyttes til. Bekymringene knyttes til usikkerhet rundt hvilke opplysninger som appene faktisk samler inn og hvordan disse opplysningene eventuelt blir viderebrukt av markedsførere og andre. Hvorfor krever for eksempel en ”lommelykt-app” tilgang til telefonens identitet?

Personopplysninger er blitt en raskt voksende handelsvare. Appene er ofte gratis eller koster bare noe få kroner. Det virkelige betalingsmiddelet vil ofte være de personopplysningene man avgir. Personopplysninger er attraktive for analyseselskap, markedsførere og annonsører. Jo mer informasjon de klarer å innhente om brukerne, jo bedre kan de skreddersy reklame til forbrukerne.

Informasjon til publikum om hvilke personopplysninger som samles inn, hva som er formålet med innsamlingen og hvordan opplysningene behandles, er avgjørende for å ivareta et godt personvern. Bakgrunnen for Datatilsynets fokus på app-markedet er at vi har inntrykk av at brukeren i liten grad informeres om hvilke personopplysninger som samles inn, samt at ansvarsforholdene mellom de ulike aktørene er uklare. Hvem er ansvarlig for at personopplysningene håndteres på en forsvarlig måte, er det app-bestilleren, app-utvikleren, app-leverandøren, eller app-brukeren selv?

1.1 Problemstilling

Siktemålet med Datatilsynets rapport er å belyse hvordan mobilapplikasjoner henter ut personopplysninger fra smarttelefoner. I rapporten ser vi også se på ansvarsforholdene i app-markedet og undersøker i hvor stor utstrekning appene er utstyrt med en personvernpolicy. Datatilsynet har ikke undersøkt hvordan opplysningene blir håndtert av appeierne og eventuelt viderebrukt av tredjeparter. Dette er eventuelt en problemstilling tilsynet vil se nærmere på i en oppfølgingsrapport.

Datatilsynet har i rapporten sett på både utenlandske og norskutviklede applikasjoner, men hovedfokus er på det norske markedet. Rapporten omhandler applikasjoner utviklet for de to største

¹ Tilsvarende undersøkelse har ikke blitt foretatt i Norge. Den amerikanske undersøkelsen er gjennomført av TRUSTe, en ledende leverandør av online personvernløsninger. http://www.truste.com/about_TRUSTe/press-room/news_truste_mobile_privacy_survey_results_2011.html

plattformene, Android og Apple/iOS. Rapporten drøfter ikke personvernrelaterte problemstillinger knyttet til operativsystemene i seg selv.

Rapporten gir i kapittel to et oversiktsbilde av de viktigste aktørene i app-markedet og omtaler særegenhetene ved de to største plattformene. Kapittel tre tar for seg de mest sentrale informasjonselementene² som applikasjonene krever tilgang til på telefonen. Kapittel fire omhandler mangelen på god informasjon til brukeren, blant annet fraværet av en personvernerklæring. I kapittel fem er fokus på de uklare ansvarsforholdene i app-markedet. I kapittel seks kommenteres kort andre juridiske utfordringer, som blant annet retten til innsyn og forholdet til annet regelverk. Avslutningsvis pekes det på de viktigste funnene i rapporten.

1.2 Metode og ressurser

Innholdet i rapporten er dels basert på egne empiriske undersøkelser og dels på eksternt kildemateriale. Datatilsynet har sett nærmere på tjue norske og tjue utenlandske Android-applikasjoner. Målsettingen med undersøkelsen har vært å kartlegge hvilke opplysninger på mobilen applikasjonene krever tilgang til og hvorvidt applikasjonene er utstyrt med en personvernpolicy. Tilsynet har valgt ut populære norske og utenlandske applikasjoner med ulike bruksområder (spill, lokasjonstjenester, værtjenester, mattjenester, nyheter, bank etc.)

Datatilsynet har kun benyttet åpent tilgjengelig informasjon i rapporten. Fokus har vært på brukerperspektivet og hvilken informasjon som er tilgjengelig for brukeren i forbindelse med nedlasting av apper. Målsetningen med rapporten har ikke vært å *”avsløre”* hvilke opplysninger appene eventuelt henter ut i det skjulte.

I utgangspunktet ønsket Datatilsynet å undersøke applikasjoner på begge de to mest populære plattformene. Android-applikasjoner er utstyrt med en relativt detaljert liste over hvilke informasjonselementer applikasjonen krever tilgang til på telefonen. Det er denne listen vi har lagt til grunn for vår analyse. iOS-plattformen er imidlertid en mer *”lukket”* plattform enn Android, og hvilke opplysninger Apple-appene krever tilgang til ligger ikke åpent tilgjengelig. I dette prosjektet har vi derfor kun studert Android-applikasjoner nærmere.

*”The App Genome Project”*³ i regi av Lookout Mobile Security har utført undersøkelser på begge plattformer, og har gjennomgått 500 000 apper så langt. Deres konklusjon er at mengden persondata som hentes ut av applikasjonene er ganske lik på Android og iOS. Det er derfor vår oppfatning at en analyse kun av Android-apper likevel gir en relativt god pekepinn på i hvor stort omfang applikasjoner samler inn data *generelt* - uavhengig av plattform. Gjennomgangen av appene ble foretatt i april og mai 2011.

Tilsynet har videre gjennomført samtaler med norske utviklere av mobilapplikasjoner. Navnet på virksomhetene er ikke nevnt i rapporten da fokus ikke var på spesifikke selskap og applikasjoner.

² Informasjonselement er enten statiske eller dynamiske opplysninger, se punkt 4.1.

³ *the App Genome Project* er verdens mest omfattende analyse av mobilapplikasjoner, der målsetningen er å få innsikt i hva applikasjonene foretar seg og å identifisere ulike potensielle sikkerhetstrusler. Prosjektet er fortsatt pågående og har pr. februar 2011 gjennomgått 500 000 Android og iOS applikasjoner. Lookout Mobile Security er et selskap som produserer sikkerhetsløsninger for smarttelefoner.

<https://www.mylookout.com/appgenome/>

Målsetningen med samtalerne har vært å få større kunnskap om, og innsikt i utviklingen av apper og å høre hvordan utviklingsmiljøene tenker rundt problemstillinger knyttet til personvern. Samtalene ble gjennomført i mai og juni 2011.

2 Kort om markedet for mobilapplikasjoner

2.1 Hva er en "app"?

Det er særlig utbredelsen av smarttelefoner som driver app-markedet. Stiftelsen Elektronikkbransjen har estimert at 70 % av alle nye mobiltelefoner solgt i 2011 vil være smarttelefoner⁴. Bruk av applikasjoner er med andre ord ikke lenger en nisjepreget aktivitet reservert unge og teknologikyndige, men noe som det brede lag av befolkningen benytter daglig.

Smarttelefoner er mobiltelefoner som tilbyr mer avansert databehandling og bedre tilkoblingsmuligheter enn tradisjonelle mobiltelefoner. En smarttelefon er i realiteten en liten håndholdt datamaskin, der man kan installere små programmer, eller applikasjoner – populært kalt app'er eller apps.

Smarttelefoner kommer med ulike operativsystem, og applikasjoner utvikles spesielt til de ulike systemene. Andre operativsystem i tillegg til Apples iOS og Googles Android er Microsofts Windows Mobile, Symbian fra Nokia og RIMs BlackBerry⁵.

Appene er tilgjengelige gjennom de ulike plattformenes app-butikker. De to største "butikkene" er Apples App Store og Googles Android Market. Veksten i antall tilgjengelige app'er i disse butikkene er enorm. Apple har godkjent 500 000 apper for salg i sin App Store og om lag 300 000 apper er tilgjengelig i Android Market⁶. Pr januar 2011 har 10 milliarder apper blitt lastet ned fra App Store⁷.

Det er utenlandske applikasjoner som dominerer listen over populære apper i Android Market og App Store, men stadig flere populære norske apper kommer på markedet. Eksempler på mye brukte norske apper er VG, Trafikanten, MatPrat, GuleSider, Wimp, Norsk TV-guide og Norsk Tipping.

2.2 Apple vs. Android

Android og Apple har svært ulik profil. Apples iPhone med tilhørende operativsystem er et lukket system, der Apple godkjenner alt fra hardware til innhold og tilgjengelig software. Android-systemet derimot, er åpent, og der står produsenter fritt til å designe egne telefoner, og innholdssiden er brukerdrevet, fri og uten forhåndsgodkjenning.

⁴ <http://www.aftenposten.no/forbruker/digital/nyheter/mobil/article4085155.ece>

⁵ RIMs BlackBerry er ikke utbredt i Norge, men dette er den mest brukte smarttelefonen i USA

⁶ Tall fra mai 2011. <http://www.nrk.no/vitenskap-og-teknologi/1.7650781>

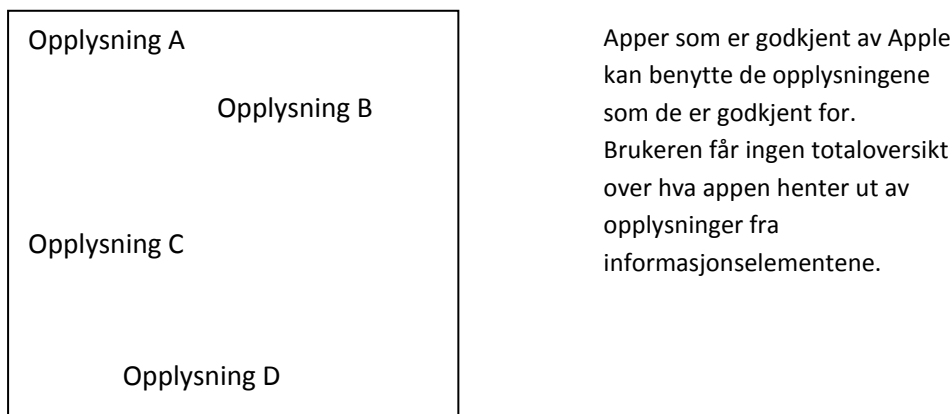
⁷ <http://www.digi.no/861028/over-60-apps-lastet-ned-per-ios-enhet>

2.2.1 Apple - iOS

Apple har streng kontroll med hvilke applikasjoner som tilbys. Hver enkelt applikasjon skal tilfredsstille kravene som Apple har fastsatt og fastsetter i henhold til sine avtaler. Dette innebærer at alle applikasjoner som tilbys blir kontrollert og godkjent av Apple. Brukeren har på forhånd, for blant annet å kunne bruke Apples App Store, akseptert Apples vilkår. Vilkårene er overordnede og gjelder generelt alle applikasjoner som blir tilbudt via App Store⁸.

Det er mulig for en iPhone-bruker å unngå Apples begrensninger når det gjelder applikasjoner. Brukeren kan da kjøre såkalt "jailbrake" på sin iPhone. Slik "åpning" av en iPhone er for de spesielt interesserte og blir ikke behandlet ytterligere i denne rapporten.

Det er i utgangspunktet ikke mulig for en iPhone-bruker å se hva en applikasjon henter ut av informasjon fra telefonen. I utgangspunktet har alle applikasjoner tilgang til alt. Apples godkjennelsesprosedyre skal imidlertid forhindre at applikasjonene foretar uønskede uthentinger av informasjon. Ettersom Apples godkjennelsesprosedyrer baseres på avtaler som Apple håndterer og ikke på europeisk eller norsk personvernlovgivning, vil det være vanskelig for brukeren å ha en klar formening om hvordan personopplysningene som hentes ut håndteres. Avtaleverket som Apple presenterer for brukeren er videre svært omfattende og vanskelig å sette seg inn i for en vanlig bruker. Apple oppdaterer og endrer også dette regelverket fortløpende. Dette gjør det utfordrende til en hver tid å vite hva som er gjeldende praksis.



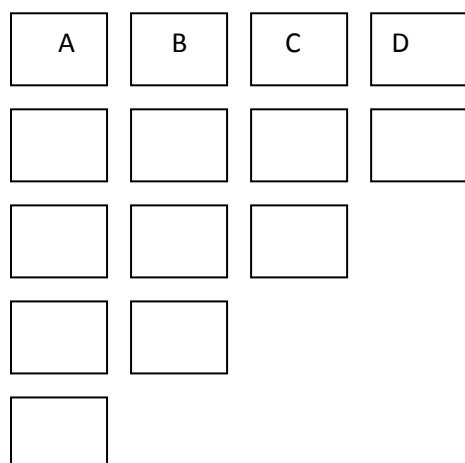
Figur 1 iOS-applikasjoner benytter opplysninger innenfor en totalramme gitt av Apple-avtale

⁸ Apple tillater at applikasjoner beregnet på spesielle lukkede grupper, som ansatte i en virksomhet, kan ha spesialtilpassede løsninger. Det er imidlertid en ganske streng håndtering av disse applikasjonene slik at ikke utenforstående skal kunne benytte dem. Slike "virksomhetsapplikasjoner" er ikke underlagt Apples godkjennelsesregime for applikasjoner.

2.2.2 Android

Android-plattformen er lagt opp på en helt annen måte enn iOS-plattformen. Det foreligger ikke en godkjennelsesordning for Android-apper (agreement⁹). Android-plattformen er basert på åpen kildekode. Utviklerne av Android-apper må imidlertid benytte forhåndsdefinerte verktøy som er gjort tilgjengelige av plattformen. Et verktøy gir tilgang til informasjon på brukerens telefon, men det er ikke mulig for verktøyet å få tilgang til denne informasjonen uten at dette gjøres kjent for brukeren. Informasjonen til brukeren blir gitt ved installasjon av applikasjonen. Brukeren kan da ta stilling til om appen skal installeres eller ikke. Det er ikke mulig for brukeren å utelate enkeltverktøy som benyttes i en app i forbindelse med selve installasjonen. Det er imidlertid i enkelte tilfeller, for enkelte verktøy, mulig å stenge for tilgangen til informasjonselementer som appen vil ha tilgang til, for eksempel GPS.

Android-plattformen benytter en såkalt "sandkaseteknologi". Dette innebærer at hver enkelt Android-app virker for seg og ikke har tilgang til opplysninger om andre installerte apper. Imidlertid vil det være mulig å få tilgang til informasjon om andre apper via lagringsområder, for eksempel SD-kortet, hvor applikasjoner kan lagre betydelig med informasjon.



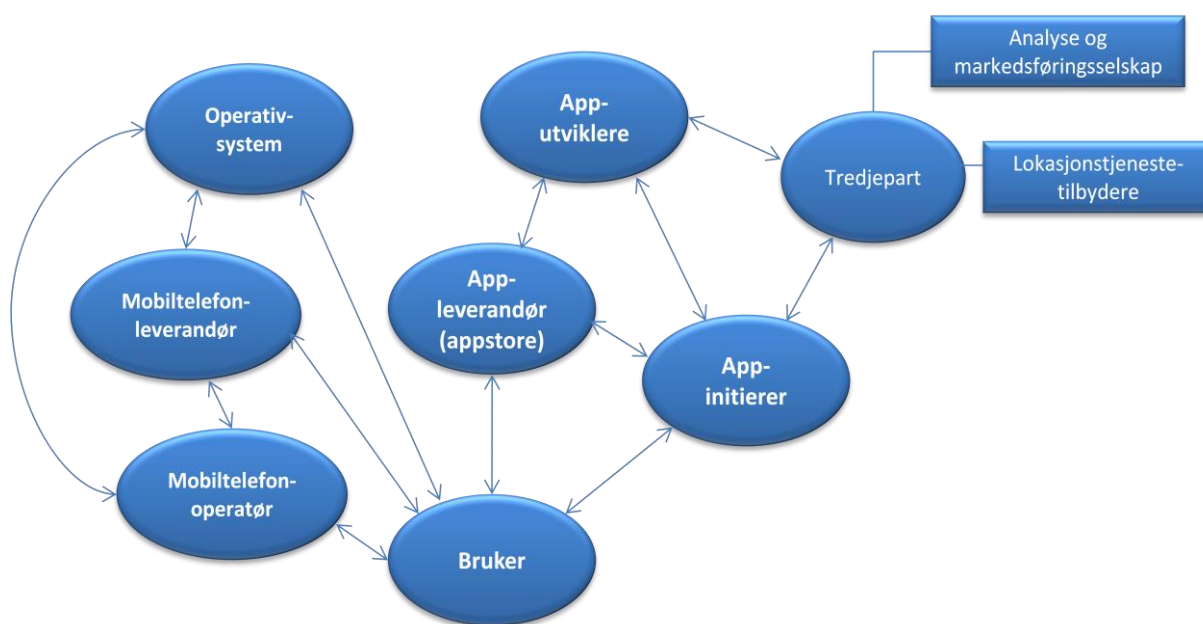
Applikasjoner som benytter Android-plattformen kan kun benytte opplysninger som det er åpnet for via utviklingsverktøyet for Android. Brukeren vil få kunnskap om hvert enkelt informasjonselement som benyttes.

Figur 2. Androidapplikasjoner vil gi tilgang til et og et opplysningselement

⁹ <http://www.android.com/us/developer-distribution-agreement.html>

2.3 Hvem skjuler seg bak en app?

Applikasjonsmarkedet er svært komplekst. "Økosystemet" appene inngår i består av mange ulike aktører, lokalisert på flere kanter av kloden. Sentrale aktører, foruten sluttbruker, er mobiltelefonleverandører, operativsystemleverandører, app-leverandører, app-utviklere, app-opppdragsgivere og diverse tredjeparter som analyseselskaper, markedsførere og leverandører av lokasjonstjenester (se figur 1).



Figur 3: oversikt over de ulike aktørene i "app-økosystemet"

2.3.1 Applikasjonsutvikler

Applikasjonsutviklerne er de som programmerer appen. Applikasjonsutviklerne er i en ekspanderende bransje. Det blir stadig flere selskaper som tilbyr applikasjonsutvikling for iPhone, Android og andre plattformer.

Det har vokst frem flere norske selskaper som lever av å utvikle applikasjoner for smarttelefoner og nettbrett. Allerede etablerte markedsførings- og internettbyråer har også opprettet egne avdelinger med fokus på app-utvikling. I tillegg utvikles mange applikasjoner fortsatt av privatpersoner.

Applikasjonsutviklerne produserer ofte appene sammen med tredjeparter som analyseselskaper, lokasjonstjenestetilbydere, annonsører og oppdragsgivere.

2.3.2 App-bestiller

Stadig flere offentlige og private aktører ser nytten av å tilby tjenester og å markedsføre seg via en mobilapplikasjon. App-bestilleren tar kontakt med en utvikler for å lage applikasjonen. Eksempler på virksomheter som har utviklet populære apper er Trafikanten, Gulesider og VG.

Rapporten diskuterer under punkt 5.1.1 de uklare ansvarsforholdene mellom app-utvikler og initiativtakeren til appen.

2.3.3 Tredjeparter

Tredjeparter kan deles inn i mange grupper. Det er reklametilbydere, analyseselskaper lokasjonstjenestetilbydere og andre som i utgangspunktet tilbyr tjenester til app-utvikleren. En analyse av 300 000 apper i regi av AppGenome Project viste at 47 % av gratis-apper på Android inneholdt tredjepartskode, mens tilsvarende prosentandel på iOS-plattformen var 23 %¹⁰.

Tredjepartskode tilbys applikasjonsutviklerne som gratistjenester de kan benytte i applikasjonene sine for ulike formål. Til gjengjeld får ofte den som leverer tredjepartskoden tilgang til analyser og statistikk eller liknende. Opplysningene kan ofte bearbeides og selges videre som analyser til markedsførere og andre som er ute etter å treffe rett målgruppe med sitt produkt.

Den største aktøren på dette markedet er *Flurry*. Flurry er en analysetjeneste som gjør det lettere for app-produsenten å se hvordan appen blir brukt. Når Flurry ligger inne i et program vil det sende fra seg detaljert informasjon om hvordan programmet brukes. Informasjonen sendes til Flurrys egen database hvor utvikleren kan logge seg på og se statistikk for sin app.

I følge en artikkel i Dagensit.no datert 26.januar 2011, sitter selskapet bak Flurry på enorme mengder informasjon om publikum som er samlet inn fra ulike apps¹¹. Flurry kan overvåke så å si all informasjon om hvordan man bruker mobilen. Brukeren opplyses generelt sett ikke om at Flurry, eller lignende tjenester, er inkludert i applikasjonen. Ansvarer til tredjepartsapplikasjoner diskuteres under punkt 6.1.2.

Det kom frem gjennom samtaler med norske app-utviklere at enkelte av selskapene har betenkeligheter med å benytte analysetjenester som Flurry i sine applikasjoner. Dette hadde blant annet sammenheng med at de er usikre på hvordan disse tredjepartsselskapene håndterer personopplysningene om norske brukere som samles inn. Et av selskapene Datatilsynet snakket med har derfor utviklet sitt eget analyseverktøy for å unngå å benytte Flurry.

2.3.4 Operativsystemleverandører og app-leverandører

Leverandører av apper (eks App Store og Android Market) samler også inn personopplysninger om brukerne. App Store krever blant annet at brukeren oppgir kredittkortnummer, selv om brukeren ikke har intensjon om å kjøpe noe fra butikken, men kun benytter seg av gratisapper. Dette gir mulighet til å identifisere brukeren.

Både på iPhone og Android blir man tilbudt apper knyttet til operativsystemet, altså apper utviklet av operativsystemleverandøren selv og ikke av tredjepart. Operativsystemleverandører vil kunne legge inn behandling av personopplysninger i operativsystemet, både for eget og andres bruk. Appene kan blant annet rapportere lokasjonsdata. Operativsystemleverandørene gir oppskrifter på hvordan man for enkelte elementers vedkommende (GPS er et eksempel på et element) kan unngå slik rapportering. Det er imidlertid likevel uklart for kunden hva slags personopplysninger som hentes ut av operativsystemleverandørens apper, om det er lokasjonsdata, kontaktdata osv.

¹⁰ <http://appadvice.com/appnn/2010/07/report-14-percent-iphone-apps-users-contact-information>

¹¹ <http://www.dagensit.no/article2066963.ece>

2.3.5 Mobiloperatørene

Mobiloperatørene, som Telenor og Netcom, lagrer personopplysninger som er nødvendige for å fakturere for tjenestene. I tillegg lagres opplysninger for å ivareta sikkerhet og drift av tjenestene, dette inkluderer blant annet lokasjonsinformasjon. Mobiloperatørene er ikke flinke til å orientere brukerne om at de lagrer slik informasjon. Datatilsynet er kjent med at dersom brukeren ber om innsyn i lagrede data vil vedkommende som regel få utlevert faktureringsdata, men ikke lokasjonsdata.

2.3.6 Mobiltelefonleverandørene

Mobiltelefonleverandørene har i sin del av operativsystemene muligheten til å selv legge inn innrapporteringer av personopplysninger. For eksempel innrapportering av lokasjonsinformasjon til leverandøren og i enkelte tilfeller identifiserende opplysninger.

3 Hva vet appene om deg?

“You should know that any data that can be gathered will be gathered”¹².

Enkelte opplysninger er mer følsomme med tanke på personvernet enn andre. Imidlertid kan alle personopplysninger oppleves følsomme når de plasseres i sammenheng med andre opplysninger, selv om hvert element alene ikke oppleves følsomt.

La oss ta et eksempel: Kari laster ned en app fra Android Market. Tjenesten er en lokasjonsbasert sosial tjeneste. Ved hjelp av den kan Kari vise vennene sine hvor hun befinner seg og hun kan få tilbud på varer i butikker i nærheten. For å kunne lokalisere Kari krever appen tilgang til lokasjonen på hennes mobiltelefon. Kari deler gjerne lokaliseringsdataene med sine venner. Det hun ikke vet er at appen, som krever tilgang til hennes kontaktliste på telefonen, deler denne informasjonen med *alle* kontaktene i denne listen. I appen ligger det også et analyseverktøy som samler inn et bredt spekter av ulike opplysninger om Kari. Opplysningene er attraktive for markedsførere og andre som ønsker å selge produkter i områder der mennesker med Karis profil oppholder seg.

For markedsførerne har opplysningene stor verdi - jo flere opplysninger de besitter, jo bedre er de i stand til å skreddersy og effektivisere sin markedsføring. Smartelefoner og apper er derfor svært verdifulle ”instrumenter” for markedsførere, ettersom de langt på vei kan betraktes som ”sensorer” for å bedrive detaljerte markedsundersøkelser om publikum.

3.1 Hvilke opplysninger henter appene ut?

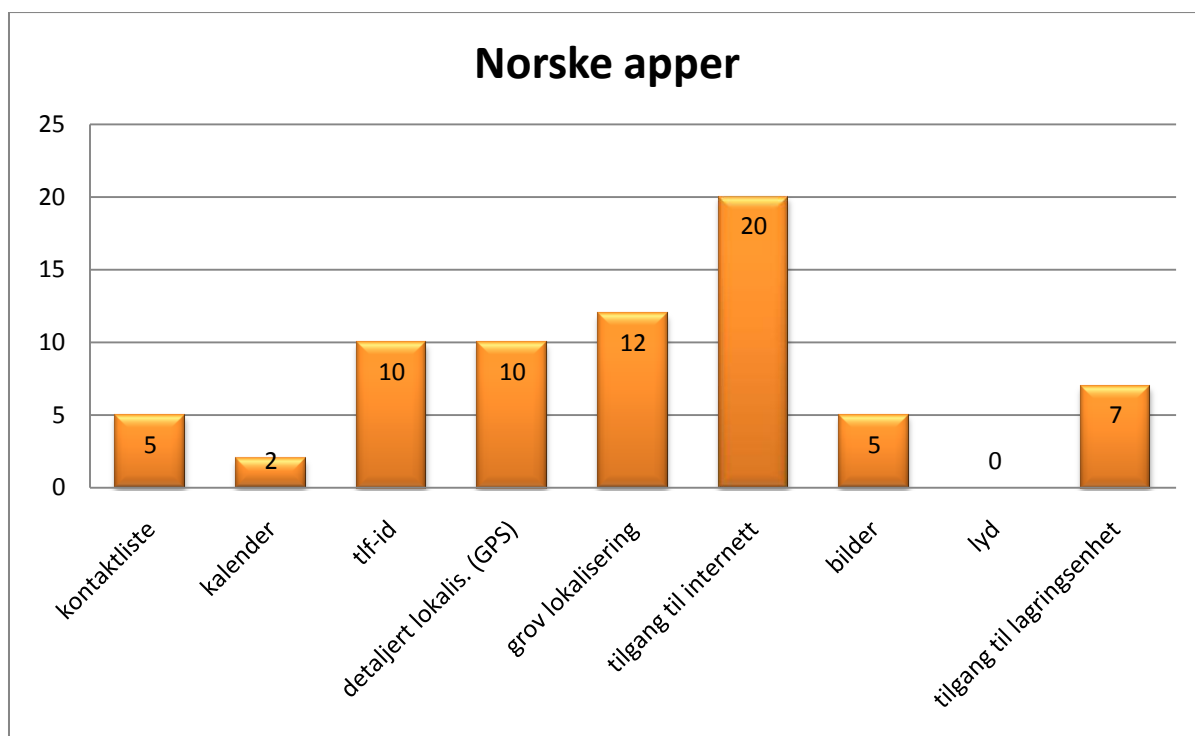
Datatilsynet har gjennomgått 20 norske og 20 utenlandske Android-applikasjoner. Tabellene nedenfor bygger på opplysninger fremkommet om hver enkelt Android-app på Android Market under fanen ”tillatelser”¹³. Som tidligere nevnt lister Android-appene opp hvilke informasjonselementer på telefonen som appen krever tilgang til. Tabellene nedenfor viser de mest

¹² “Snooping: It’s not a crime, it’s a feature”, av Mark Elgan i Computerworld, 16. April 2011

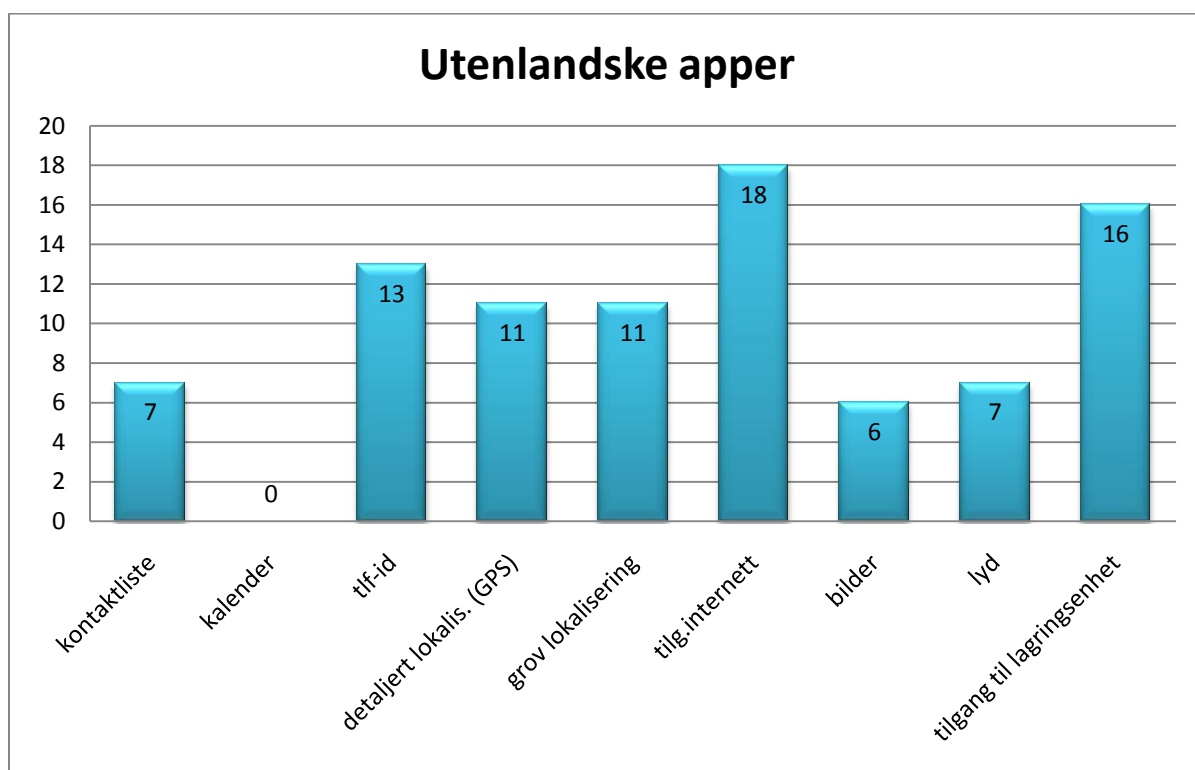
http://www.computerworld.com/s/article/9215853/Snooping_It_s_not_a_crime_it_s_a_feature?taxonomyId=84&pageNumber=2

¹³ Se vedlegg 4

sentrale informasjonselementene. En fullstendig oversikt over alle opplysningene som appene krever tilgang til finnes i vedlegg 5:



Tabell 1: Oversikt over hvilke opplysninger 20 norske Android-apper oppgir at de krever tilgang til



Tabell 2: Oversikt over hvilke opplysninger 20 utenlandske (i hovedsak amerikanske) Android-apper oppgir at de krever tilgang til

Opplysningene appen krever tilgang til på smarttelefonen kan deles inn i to hovedgrupper. Det ene er opplysninger som er statisk lagret på mobilen og det andre er opplysninger som produseres kontinuerlig av mobilens hardware (maskinvarekontroller).

Eksempler på statisk lagrede opplysninger er:

- Identifiserende opplysninger (se 4.1.2)
- Kontaktdata (se 4.1.3)
- Tekst (ukryptert tekst, for eksempel notater)

Eksempler på dynamiske opplysninger er:

- GPS-, WiFi-, basestasjons-lokasjon (se 4.1.1)
- Opplysninger fra kamera (se 4.1.5)
- Lyd fra mikrofon (se 4.1.5)
- Data fra gyroskop og akselerometer, bevegelsessensor, X,Y og Z akser (se 4.1.6)

3.1.1 Lokasjonsdata

Lokasjonsopplysninger er en viktig og mye brukt informasjonskomponent for de ulike aktørene i app-markedet. Halvparten av appene vi har sett på innhenter denne typen data.

Lokasjonsdata er i denne sammenheng ofte ansett som en av de mest følsomme opplysningene som innhentes om oss. Ettersom mobiltelefonen er tett knyttet til eieren sin vil lagring av bevegelsesmønsteret til telefonen gi svært detaljert innsikt i privatlivet til eieren. Mobiltelefonen er sjelden noe vi legger fra oss, og lokasjonsmønsteret som lagres om den enkelte vil derfor langt på vei være komplett.

Lokasjonen kan innhentes på minst tre måter:

- GPS: gir en meget nøyaktig stedsangivelse på noen få meter.
- WiFi: kan gi en meget nøyaktig stedangivelse i tettbebygget strøk, med nøyaktighet på under 100 meter.
- Basestasjonsinfo: kan gi en ganske nøyaktig stedsangivelse i tettbebygget strøk, med en nøyaktighet ned til 100 meter.

GPS og WiFi-elementet kan skrus av fra brukers side. Basestasjonsinformasjonen er imidlertid vanskeligere å skru av, da dette vil stenge for ordinær kommunikasjon med mobilen.

På iOS-plattformen er det mulig å skru av innhenting av GPS-lokaliseringen spesifikt for enkelt-applikasjoner. Hvorvidt dette også forhindrer bruk av IP-lokalisering via Wifi eller lokalisering via basestasjon, gjøres ikke klart for brukeren. På Android-plattformen er det mulig å skru av innhenting av GPS-data generelt, men det samme spørsmålet er gyldig som for iOS, om brukeren kan være sikker på at bruk av IP-lokalisering via Wifi eller lokalisering via basestasjon også er utelukket. Det er så langt tilsynet kjenner til ikke mulig for brukeren å sikre seg mot at ikke noen av de ulike alternativene for å fastslå lokasjon benyttes. Brukeren er heller ikke informert om hvordan lokasjonsdataene som innhentes håndteres og eventuelt viderebrukes av aktørene i det tidligere nevnte økosystemet.

Art 29 gruppen, som er sammenslutningen av personvernmyndigheter i EU, har publisert en egen opinion om lokasjonstjenester på smarttelefoner¹⁴. Dette dokumentet konkluderer med at aktører som ønsker å benytte lokasjonsdata må innhente aktivt samtykke fra brukeren.

3.1.2 Identifiserende opplysninger

Det er vanlig å be om identifiserende opplysninger for å kunne opprette kommunikasjonen med appbrukeren. Typiske identifiserende opplysninger er: navn, adresse, mobilnummer, e-postadresse, IP-adresse, IMEI-nummer¹⁵, kredittkortinformasjon og kontonummer. Omlag halvparten av de 40 applikasjonene rapporten har gjennomgått innhenter identifiserende opplysninger.

Opplysninger som unikt kan identifisere brukeren har stor verdi for mange av aktørene i app-markedet. Slike opplysninger er interessante fordi de kan benyttes til mange andre innbringende formål enn det opprinnelige. For eksempel er de svært verdifulle med henblikk på å utarbeide gode profiler på kundemassen. Mange aktører vil derfor være lite interessert i å slette slike data. Innenfor europeisk lovgivning er det satt klare krav til håndtering av denne typen data. I amerikansk lovgivning derimot er dette mer uklart.

Brukere som benytter en applikasjon som krever tilgang til identifiserende opplysninger vil, slik det fungerer i dag, ha svært liten kontroll over hvordan disse opplysningene brukes og eventuelt videreformidles av andre aktører.

I PC-markedet har det vært en høy bevissthet knyttet til innsamlingen av identifiserende opplysninger, og at det skal være mulig å unngå bruk av slike¹⁶. Det norske ekom-regleverket regulerer blant annet bruken av cookies¹⁷. Det har i app-markedet så langt ikke vært et tilsvarende fokus på viktigheten av anonymitet.

3.1.3 Kontaktopplysninger

Kontaktopplysninger kan bestå av enormt mange informasjonselementer. Det blir for omfattende å liste disse opp her. Grunnleggende kontaktdata er e-postadresser, navn og telefonnummer. Videre vil også følgende data kunne komme inn som kontaktopplysninger: fødselsdato, ansettelsesforhold, interesser, familie og vennerelasjoner. Det er i flere sammenhenger relevant for en applikasjon å hente ut kontaktopplysninger eller legge til kontaktopplysninger på brukerens smarttelefon.

Applikasjonens innhenting av kontaktopplysninger på telefonen omfatter ikke bare appbrukeren selv, men også de kontakter denne har registrert i sin mobiltelefon. Enkelte aktører henter ut hele kontaktlisten. Appene ber om samtykke til å gjøre dette, men det er ikke alltid lett for brukeren å få med seg at samtykke gis, eller hva samtykket i realiteten innebærer.

Kontaktopplysninger kan ikke bare betraktes isolert som enkeltdata om brukeren. Kontaktdata er interessant fordi det forteller noe om relasjoner. Det vil si at dataene forteller noe om brukeren og vedkommendes forhold til verden rundt seg (venner, interesser, jobb). De som står bak applikasjoner

¹⁴ Opinion 13/2011 on Geolocation services on smart mobile devices

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

¹⁵ IMEI er en forkortelse for International Mobile Equipment Identity og er et slags serienummer for telefonen

¹⁶ Eksempel: Microsoft Media Player-sak fra 2002

<http://www.wired.com/politics/security/news/2002/02/50567> og <http://news.cnet.com/2100-1023-955514.html>

¹⁷ Ekomforskriften § 7-3: <http://www.lovdatab.no/for/sf/sd/td-20040216-0401-008.html#7-3>

for sosiale nettsteder er spesielt interessert i denne typen data, det samme er virksomheter som driver markedsføring. Jo mer konkrete data som er tilgjengelige, særlig de som appbrukerne legger inn selv på telefonen, har høy verdi.

3.1.4 Kalenderdata

Noen applikasjoner skriver til kalender eller henter kalenderdata. Kalenderopplysninger vil ikke bare kunne vise aktiviteter, men også fremtidig og historisk reisevirksomhet (lokasjon), samt relasjoner. Ved for eksempel synkronisering mot arbeidsgivers kalender, vil det være mulighet for at kalenderoppføringen også vil bli synlig for arbeidsgiver, kollegaer, samt andre aktører med tilgang til arbeidsgivers kalender, uten at brukeren nødvendigvis er klar over at dette skjer.

3.1.5 Kamera og mikrofon

Kamera og lydaktivering håndteres under hardware (maskinvarekontroller). Applikasjoner som har tilgang til kameraet vil benytte dette når appbrukeren ber om det. Det vil kunne være nødvendig å gi applikasjonen tilgang til kamera for å kunne håndtere andre elementer, som for eksempel lys/blits. Enkelte apper aktiverer imidlertid kameraet uten at brukeren informeres om det. Det samme gjelder lyd. Den amerikanske bilde-delingsappen "Color App" er trukket frem av mediene som et eksempel på en app som aktiverer mikrofonen uten at brukeren informeres om dette¹⁸. I dette tilfellet er det heller ikke naturlig for brukeren å anta at appen vil ta opp lyd, da formålet med tjenesten er å dele bilder.

3.1.6 Gyroskop og akselerometer

Gyroskop og akselerometer er hardwarekontroller som kan fortelle mye om appbrukeren. Enhetene er kanskje synligst i forbindelse med spillapplikasjoner. Enheten registrerer berøring for å gjennomføre aktiviteter på smarttelefonen, for eksempel hoppe til neste melodi i musikkspilleren. Det er også mulig å la enheten rapportere om bevegelse til andre og tredjeparter. Enhetene er så nøyaktige at de kan fortelle mye om hva appbrukeren gjør i øyeblikket. Om du sitter i ro, går eller jogger. Den kan også via gjenkjennelse gi indikasjoner på om du spiser eller kjører buss. Det er videre utviklet apper som kan rapportere om brukerens søvnmonster, ved at man legger mobilen i sengen. Det foreligger arbeid om ganglagsbiometri (Nislab ved HIG og ganglagsbiometri) som kan skille mellom personer på grunnlag av mobilens bevegelsessensorer.

Gyroskop og akselerometer vil kunne få stor betydning fremover når disse funksjonene blir mer aktivt tatt i bruk. Funksjonene er særlig interessante i forbindelse med identifisering av personer og aktiviteter. I likhet med lokasjonsinformasjon vil disse funksjonene ha spesiell viktighet for personvernet.

¹⁸ http://www.computerworld.com/s/article/9215853/Snooping_It_s_not_a_crime_it_s_a_feature

4 Mangel på kontroll og oversikt

4.1 System basert på tillit

Ved installasjon og bruk av en app vil brukeren i større eller mindre grad gi appen tilgang til opplysninger lagret på mobilen, eller hentet fra hardware på mobilen. Brukeren må ved nedlasting av appen ta stilling til om han tror at personopplysninger vil bli håndtert på en akseptabel måte. Ettersom brukeren har begrenset mulighet til å vite hvilke opplysninger som samles inn, hvordan de håndteres og hvem som er ansvarlig, baseres denne transaksjonen i stor grad på tillitt til de ulike app-aktørene.

Brukere av iPhone overlater håndteringsnivået for personopplysningene sine til Apple, som gjennom forhåndsgodkjenning av alle apper garanterer at disse oppfyller bestemte krav. Fra et brukerståsted kan man sammenligne iOS-plattformens håndtering av personopplysninger som å åpne en låvedør inn til telefonen (illustrert i figur 1). Når først låvedøren er åpnet vil brukeren ikke vite sikkert hvilke opplysninger som går igjennom den, men må velge å stole på at Apple har full kontroll over appene og hva disse kan hente ut, dvs at Apple passer på hvem som har tilgang til de opplysningene som passerer låvedøra. Det er vanskelig for iPhone-brukeren på egenhånd å vurdere hvorvidt man kan stole på en app, ettersom det ikke opplyses hvilke opplysninger som hentes ut og hvem som er ansvarlig for appen. Systemet er altså basert på brukerens tillitt til Apple.

Android-brukeren er i større grad enn iPhone-brukeren overlatt til egne vurderinger om hvorvidt en app vil håndtere personopplysningene forsvarlig eller ikke. Android tar ikke ansvar for at appene oppfyller visse minstekrav knyttet til dette. Brukeren må, før man foretar installasjon, vurdere hvorvidt appen skal få tilgang til de informasjonselementene den lister opp. Brukeren må blant annet vurdere om tillatelsen for tilgang er nødvendig og tilfredsstillende egne krav til trygghet for de personopplysningene man avgir. Android-brukeren må også ta stilling til om personen eller virksomheten som leverer appen er tillitvekkende. Det er ikke alltid lett å se hvem som står ansvarlig for en app.

Androids håndtering av personopplysninger kan illustreres som det å åpne veldig mange luker (illustrert i figur 2), i motsetning til Apple hvor man åpner én stor dør. Når lukene først er åpnet vil brukeren imidlertid ha liten kontroll med hva som går igjennom dem. Her er ingen annen autoritet som passer på. Brukeren kan la være å installere applikasjoner som ser ut til å åpne luker (åpne for informasjon) som brukeren ikke ønsker å gi applikasjonen tilgang til. En Android-bruker vil, sammenlignet med iPhone-brukeren, kunne foreta en litt mer kvalifisert vurdering av hver enkelt applikasjon før nedlasting. Likevel må Android-brukeren også basere installasjonen av appen på tillitt. Man må som bruker ha tillitt til at de ulike aktørene faktisk ikke misbruker de opplysningene det er gitt tilgang til på telefonen.

4.2 Fravær av informasjon

Personopplysningsloven gir borgeren rettigheter i de tilfeller en virksomhet behandler opplysninger om vedkommende. Forutsetningene for utøvelse av disse rettighetene er at vedkommende er kjent med at det foregår en behandling og at vedkommende er kjent med rettighetene sine. Informasjon om at det skjer en behandling er spesielt viktig i de tilfeller det ikke er intuitivt for borgeren at så

skjer. Det følger av personopplysningslovens § 19 at kunden skal informeres om blant annet formålet med behandlingen av personopplysningene, om opplysningene vil bli utlevert til en tredjepart, m.m.

Ved å utarbeide en personvernerklæring vil virksomheter som lager applikasjoner sette brukerne bedre i stand til å sikre sine rettigheter etter personvernlovgivningen. En god personvernerklæring er noe app-leverandører vil tjene på ved at den kan føre til bedre tillit mellom virksomheten og brukeren.

En personvernerklæring kan legges enten i selve appen eller på Android market og App Store. En fordel med å la informasjonen være tilgjengelig på Android Market og App Store er at den da er tilgjengelig for brukeren før vedkommende foretar installasjon av appen. Ved å installere appen vil brukeren gi et underforstått samtykke til håndtering av personopplysninger. Det er derfor avgjørende at brukeren får tilgang til nødvendig informasjon *før* appen installeres. Dersom informasjonen utelukkende ligger i selve appen, vil brukeren informeres *etter* at samtykke er gitt – dette er feil rekkefølge. *Fordelen* ved å la informasjon også være tilgjengelig i appen er at den da lett vil kunne hentes frem dersom brukeren senere lurer på hvordan håndteringen av personopplysninger gjøres. Dette kan medføre at brukeren ønsker å trekke samtykket tilbake ved å avinstallere appen.

Det vil være positivt for brukeren om informasjon om appens håndtering av personopplysninger også ligger på virksomhetens ordinære nettside. Dette fordi tilgjengeligheten til informasjonen blir bedre og fordi det kan bidra til å synliggjøre hvem som er ansvarlig for appen. En personvernerklæring på hjemmesiden til app-ansvarlig vil også kunne tydeliggjøre om applikasjonen faller inn under norsk lovgivning, spesielt med tanke på at appene lastes ned fra internasjonale aktører som for eksempel Apple og Android.

Av de 20 norske Android-appene Datatilsynet har sett på, er det ingen som har en lett tilgjengelig personvernerklæring, verken i appen, på Android Market eller på app-eierens nettsted. Utfordringen med å finne god og relevant informasjon om hvem som er ansvarlig for appen, og hvordan den håndterer personopplysninger, kan vises ved følgende illustrerende eksempel:

Trafikantappen for Android opplyser i forbindelse med nedlasting fra Android Market at den håndterer følgende opplysninger:

- Din Plassering, detaljert (GPS) plassering, grov(nettnetbasert) plassering
- Nettnetkommunikasjon, full Internett-tilgang
- Din personlige informasjon, les kontaktdata
- Systemverktøy, endre Wi-Fi-tilstand, hindre telefonen i å deaktiveres
- Nettnetkommunikasjon, vis nettnetstatus, vis Wi-Fi-status
- Maskinvarekontroller, kontroller vibrator

Flere av disse er å anse som personopplysninger.

Ved installasjonstidspunktet av Trafikanten for **Android** blir det gitt enkelte tilleggsopplysninger på engelsk. Det blir blant annet opplyst at det innhentes kontaktdata for å kunne lokalisere brukerens kontakter. Dette gjøres for at brukeren skal kunne ledes til stoppesteder nærme sine venner. Det blir videre opplyst at appen kun har tilgang til GPS-data.

I selve appen Trafikanten for Android blir det opplyst at appen er utviklet av en privatperson i samarbeid med Trafikanten. Det er ikke opplyst hvem som er ansvarlig for håndteringen av personopplysninger. Alle feilmeldinger og tilbakemeldinger skal gå via denne privatpersonens gmail-konto.

I Trafikantens app for **iPhone** er det ikke gitt informasjon om hvem som er ansvarlig for håndtering av personopplysningene, men det er vist til at man kan få mer informasjon på trafikanten.no. Videre er det vist til copyright for Trafikanten AS og Shortcut AS.

Ved installasjonstidspunktet for Trafikanten for **iPhone** blir det ikke gitt informasjon om håndtering av personopplysninger. Heller ikke dersom man går videre til utviklerens nettsted som det linkes til.

På Trafikanten.no ligger det litt informasjon om virksomhetens apper for iPhone og Android. Det opplyses imidlertid ikke her om hvordan personopplysninger som innhentes i forbindelse med bruk av appene håndteres. I personvernerklæringen for trafikanten.no vises det utelukkende til hvordan selve nettstedet håndterer personopplysninger, appene er ikke nevnt. Ved installasjon av Trafikantappene vil følgelig ikke brukeren vite hvordan egne personopplysninger håndteres og hvem de håndteres av.

Eksempelet med Trafikanten viser at det er mulig å informere brukeren på flere ulike steder: på App Store og Android Market, i appen eller på nettstedet til appansvarlig. Muligheten til å informere brukeren benyttes imidlertid sjelden.

5 Uklare ansvarsforhold

For brukeren er det viktig å vite *hvem* som er behandlingsansvarlig for de personopplysningene som samles inn. Uten denne kunnskapen kan ikke brukeren utøve sine rettigheter etter personopplysningsloven. Brukeren kan blant annet ikke kontrollere at opplysningene blir behandlet på korrekt måte, at det ikke lagres flere opplysninger enn nødvendig, og at opplysningene blir slettet straks de ikke lenger er nødvendige for behandlingen.

Som vist under punkt 3.3 består app-markedet av en lang rekke ulike aktører. For en bruker vil det være en vanskelig oppgave å be om innsyn hos alle de ulike aktørene for å forsikre seg om at ens personopplysninger blir behandlet korrekt.

En sentral utfordring er app-markedets globale karakter. App-utviklere tilbyr sine produkter på globale plattformer, hvor forbrukere uavhengig av geografiske grenser kan laste dem ned. Det enorme utvalget av applikasjoner, laget av utviklere plassert over hele verden, men tilgjengelige i felles globale app-butikker, gjør det uklart for forbrukerne under hvilket lands lovverk de ulike appene faller inn.

Dersom appen forholder seg til amerikansk lovverk vil dette kunne avvike betydelig fra norsk lov og det europeiske personverndirektivet. Krav som anses som opplagte i Norge og Europa er ikke like opplagt for et selskap under amerikansk lovgivning. Med bakgrunn i disse forskjellene har EU og USA

etablert en særavtale som regulerer overføring av personopplysninger, Safe Harbor-avtalen¹⁹. Formålet er å få amerikanske behandlingsansvarlige til å tilfredsstille kravet til et ”tilstrekkelig vernnivå” i direktivets art. 25 (1), som tilsvare personopplysningsloven § 29. Safe Harbor-avtalen gjelder kun overføring av personopplysninger fra et EU-/EØS-land til USA.

Apper som leveres via App Store skal i utgangspunktet forholde seg til amerikansk lov samt de vilkår som Apple har satt. Applikasjoner initiert av norske aktører med norske borgere som målgruppe må imidlertid også forholde seg til den norske personopplysningsloven. Hvordan appene, inkludert tredjeparter forholder seg til norsk lovverk vil måtte avklares av appansvarlige (eventuelt behandlingsansvarlig dersom det behandles personopplysninger) for alle aktuelle plattformer, iOS, Android osv.

5.1 Hvem er behandlingsansvarlig?

Det er viktig å få klarlagt hvem som er den behandlingsansvarlige for hver enkelt applikasjon²⁰. Den behandlingsansvarlige får blant annet en opplysningsplikt med hensyn til hvordan man håndterer personopplysninger. Det er viktig at behandlingsansvaret plasseres i hvert enkelt tilfelle, på bakgrunn av formålet med innsamlingen av personopplysningene og kontraktsmessige forhold mellom partene.

5.1.1 Forholdet mellom utvikler og oppdragsgiver

Applikasjonsutvikleren programmerer appen og er den som i utgangspunktet har størst innsikt i hvordan applikasjonen håndterer personopplysninger. Applikasjonsutvikleren vet hvilke tredjeparter som er innblandet i nærmeste ledd til appen, slik som for eksempel analyse og statistikkvirksomheter, lokasjonsselskaper og markedsførere.

Mange app-utviklere er små organisasjoner, som ofte mangler ressurser eller den nødvendige kunnskap til å sette seg inn i personvernlovgivningen eller hvordan dette blir håndtert av plattformene de laster appene opp på. Plattformene har en viktig rolle å spille for å sikre kundene et godt personvern, men app-utviklerne må være ansvarlig for sin egen praksis – de kan ikke lene seg på plattformen og regne med at man der tar ansvaret for god sikkerhet og personvern.

Særlig i det norske app-markedet utvikles applikasjoner oftest på vegne av en oppdragsgiver. 13 av de 20 norske applikasjonene som Datatilsynet har sett på i denne rapporten er utviklet på bestilling. Det er oppdragsgiver som setter premisser for appen og det er i utgangspunktet naturlig at vedkommende virksomhet da er behandlingsansvarlig for håndteringen av personopplysninger. Utfordringen for oppdragsgiveren er at det kan være vanskelig for å få et fullstendig bilde av hvordan applikasjonsutviklerne har lagt håndteringen av personopplysninger og hvilke tredjeparter som er involvert i appen (jf punktet over). Det kan derfor være utfordrende for oppdragsgiver å skrive en god personvernpolicy for sine brukere.

¹⁹ http://www.datatilsynet.no/templates/article____2626.aspx

²⁰ En behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysningene og hvilke hjelpemidler som skal brukes. En databehandler behandler personopplysninger på vegne av den behandlingsansvarlige.

Oppdragsgiver har ofte et ønske om å få tilgang til personopplysningene som samles inn av applikasjonen, fordi disse opplysningene forteller dem hvem kundene er og hvordan de benytter applikasjonen. Dersom utvikleren "drifter" appen og behandler personopplysninger på vegne av oppdragsgiveren, skal det foreligge en databehandleravtale.

Det ikke alltid at den som fremstår som oppdragsgiver faktisk har tatt initiativ til å lage en app. De som fremstår som oppdragsgivere kan ha fått tilbudt en app av en apputvikler. Utvikleren kan ha fått tillatelse til å benytte logoer og navnet til et selskap, gjerne i overensstemmelse med selskapet, men uten at noen nødvendigvis tar konkret ansvaret for appen. Det kan være utviklere som har egen økonomisk eller annen interesse av å etablere en app med andres logo.

5.1.2 Forholdet til tredjeparter

Tredjeparter kan som nevnt i punkt 3.3.3 deles inn i mange grupper. Det kan være analyseselskaper, markedsførere og lokasjonstjenestetilbydere som i utgangspunktet tilbyr tjenester for app-utviklere. Den som er behandlingsansvarlig kan i utgangspunktet ikke overlate personopplysninger fra applikasjonen til tredjeparter uten at det er etablert en databehandleravtale i henhold til personopplysningslovens § 15.

Vanligvis utfører databehandler en betalt tjeneste for behandlingsansvarlig. I app-verdenen er det som tidligere nevnt ofte ikke vanlig å ta betalt i form av penger for tjenestene som tilbys. Betalingsmiddelet kan også være personopplysninger. Dette medfører at tredjeparter ikke bare leverer tjenester til app-ansvarlig som databehandler, men at de også håndterer og videreformidler personopplysninger på selvstendig grunnlag. Dersom det overlates personopplysninger til tredjeparter for tredjepartens eget formål, vil tredjeparten selv måtte være behandlingsansvarlig og forholde seg til norsk lov.

Mange av de mye brukte tredjepartsleverandørene agerer utenfor norsk og europeisk lovverk. Ofte benytter selskapene standardkontrakter overfor de øvrige aktørene uten at det orienteres om selskapenes videre håndtering av personopplysninger for eget formål. Det er viktig at de som er involvert i utviklingen av apper, både app-utviklere og oppdragsgivere av appen, ser denne todelingen og tar nødvendige grep for å få kontroll over den videre behandlingen av personopplysninger foretatt av tredjeparter.

6 Andre juridiske spørsmål

6.1 Avtale er utgangspunktet

Etter personopplysningsloven må det i utgangspunktet foreligge et behandlingsgrunnlag, et rettslig grunnlag, for enhver behandling av personopplysninger. De vanligste rettslige grunnlagene er at behandling av personopplysninger enten er hjemlet i lov eller at behandlingen er basert på et aktivt samtykke fra den registrerte. I henhold til personopplysningsloven skal den behandlingsansvarlige bare benytte personopplysningene til uttrykkelig angitte formål som er begrunnet i virksomheten. Personopplysningene skal ikke benyttes til senere formål som er uforenlige med det opprinnelige formålet med behandlingen, uten at den registrerte samtykker til dette.

Ved kjøp av tjenester og produkter, som også forutsetter at noen personopplysninger blir innhentet og brukt, vil det rettslige grunnlaget normalt finnes i personopplysningslovens § 8 bokstav a). I følge denne bestemmelsen kan personopplysninger behandles, altså innhentes og brukes, når dette er nødvendig for å *oppfylle en avtale* med kunden. Grunnen til at avtale-alternativet, i hvert fall som et utgangspunkt, er det mest aktuelle for apper, er at behandlingen av personopplysninger ofte vil være nødvendig for å oppfylle avtalen med kunden. Avtalen i seg selv vil derimot ikke i hovedsak dreie seg om selve behandlingen av personopplysningene, men om å få et produkt eller en tjeneste.

Personopplysningslovens § 8 bokstav a) sier at den behandlingsansvarlige har lov til å behandle personopplysninger om kunden som er nødvendige for å oppfylle avtalen med vedkommende. Dette setter begrensninger på hvor mange personopplysninger den behandlingsansvarlige kan innhente og bruke i medhold av dette rettslige grunnlaget – innhenting og bruken må på en eller annen måte være nødvendig for å oppfylle avtalen. Dersom det innhentes og brukes personopplysninger ut over det som er nødvendig for å oppfylle avtalen, må det foreligge et nytt rettslig grunnlag for dette. Det mest naturlige vil være at det innhentes et samtykke fra kunden for innhenting og bruk av personopplysninger ut over det som er nødvendig for å oppfylle avtalen.

Det vil trolig ofte oppstå et spørsmål om hvilke opplysninger som strengt tatt er nødvendige for å oppfylle avtalen, og ikke minst hvem som skal vurdere nødvendigheten av dem. Til en viss grad er det opp til den behandlingsansvarlige å vurdere hva virksomheten trenger for å oppfylle avtalen, men man vil måtte ta et standpunkt til om virksomhetens vurdering er rimelig og fornuftig.

6.2 Retten til innsyn og informasjon

På grunn av de uklare ansvarsforholdene i app-markedet, vil en app-bruker ikke ha en enkel oppgave med å be om innsyn i personopplysningene som de forskjellige virksomheter håndterer.

Både i forbindelse med avtale og samtykke som et rettslig grunnlag for behandling av personopplysninger, er det en forutsetning at kunden får informasjon om hvordan hans eller hennes personopplysninger skal behandles. At kunden skal vite hvilke opplysninger som innhentes og brukes, følger av selve forutsetningen til behandlingsgrunnlaget – man kan ikke inngå en avtale eller samtykke til noe man ikke kjenner til innholdet av. Innsynsretten følger også av personopplysningslovens § 18. Det følger i tillegg av personopplysningslovens § 19 at kunden skal

informeres om blant annet formålet med behandlingen av personopplysningene, om opplysningene vil bli utlevert til en tredjepart, m.m.

Personopplysningslovens § 21 kan også være relevant i dette tilfellet dersom personopplysninger behandles til det formål å lage personprofiler. Dersom det innhentes og lagres personopplysninger i forbindelse med kjøp og bruk av en app, vil kunden ha krav på innsyn i alle opplysninger som er lagret om han eller henne. Denne bestemmelsen er å forstå slik at den som kjøper en app blant annet har krav på innsyn i hvilke typer personopplysninger som behandles, formålet med behandlingen av personopplysningene og om opplysningene utleveres til tredjeparter.

En kunde har anledning til å kontakte for eksempel den ansvarlige for Trafikant-appen og i henhold til loven kunne kreve at alle opplysninger som ligger lagret i forbindelse med vedkommendes bruk av Trafikant-appen skal utleveres.

I henhold til personopplysningsloven skal behandlingsansvarlig for en applikasjon som håndterer personopplysninger opplyse om:

- Hvem som er behandlingsansvarlig for appen
- Formålet med behandlingen av personopplysninger
- Hvilke personopplysninger som håndteres
- Om personopplysninger vil bli utlevert og eventuelt hvem som er mottaker
- Om sletting av personopplysningene
- Sikkerhetstiltak
- Annet som gjør den registrerte i stand til å bruke sine rettigheter.
- Hvilket lovverk (jurisdiksjon) appens håndtering av personopplysninger ligger inn under

6.3 Forholdet til annet lovverk

Når privatpersoner kjøper produkter eller tjenester, reguleres dette vanligvis av annen lovgivning enn personopplysningsloven. Når det gjelder selve kjøpet av en app til en mobiltelefon, vil denne transaksjonen etter norsk rett i hovedsak reguleres av forbrukerkjøpsloven (så fremt denne får anvendelse av hensyn til lovens geografiske begrensninger). Formålet med transaksjonen er å motta et produkt (et spill, værtjeneste eller lignende) – hovedformålet med transaksjonen er altså ikke at den behandlingsansvarlige skal behandle personopplysninger om kunden. Sett fra kundens ståsted er dette en bi-effekt.

Også forbrukerkjøpsloven har bestemmelse om manglende informasjon om produktet. Et produkt regnes i følge loven å ha en mangel dersom selgeren ved kjøpet har forsømt å opplyse om vesentlige forhold ved produktet som kunne ha antas å ha virket inn på kjøpet.

7 Konklusjon

Datatilsynet konkluderer med at:

- App-brukeren er ikke i tilfredsstillende grad informert om *hvilke* opplysninger som samles inn om vedkommende, hva som er *formålet* med innsamlingen og hvordan opplysningene eventuelt *viderebrukes*.
- Det fremstår som uavklart hvem som er behandlingsansvarlig for applikasjoner som behandler personopplysninger.
- App-brukerens *rett til innsyn* i personopplysningene som behandles er vanskelig når det ikke fremkommer hvem som håndterer personopplysningene (hvem som er behandlingsansvarlig).
- Muligheten til å legge ut informasjon om hvordan appen håndterer personopplysninger i App Store eller Android Market, benyttes sjelden. Dersom dette i større grad hadde blitt gjort ville brukeren før installasjonstidspunktet hatt et bedre grunnlag til å ta en kvalifisert beslutning om å installere appen eller ikke.
- Muligheten til å legge ut informasjon i selve appen om hvordan den håndterer personopplysninger, benyttes sjelden. Det er verdifullt å legge ut informasjon også her slik at brukeren har den lett tilgjengelig også etter at applikasjonen er lastet ned. Dersom informasjonen *utelukkende* ligger i selve appen, vil imidlertid brukeren først informeres *etter* at samtykke i forbindelse med nedlasting av appen er gitt – dette er feil rekkefølge.
- Muligheten til å legge ut informasjon om hvordan appen håndterer personopplysninger på nettsiden som app-ansvarlig råder over, benyttes sjelden. Dette er uheldig, ettersom en slik personvernerklæring ville økt tilgjengeligheten til informasjonen og fordi det ville bidratt til å synliggjøre hvem som er ansvarlig for appen. Det ville også ha klargjort hvilket lovverk (jurisdiksjon) appens håndtering av personopplysninger ligger inn under.

8 VEDLEGG

Vedlegg 1: Norske Android-apper gjennomgått i rapporten.

Applikasjoner Android	Om tjenesten		
Norske	Ansvarlig/bestiller	Utvikler	Betaling eller gratis
DNB Nor eiendom	DNB Nor (usikkert)	avantime.se	gratis
Nordea	Nordea (usikkert)	nordea.no	gratis
Fokus Mobilbank	Fokus Bank	(ikke klart)	gratis
Gulesider	Eniro	(ikke klart)	gratis
Matprat	Opplysningskontoret for egg og kjøtt	SmartpPhones Telecom AS	gratis
YR.no Widget	Øystein Gulliksen	Øystein Gulliksen	gratis
Wimp	Aspiro Music	Aspiro Music	gratis
Trafikanten offisiell	(ikke klart)	Anders Aagard	gratis
TV 2 Sporten	TV 2	(ikke klart)	gratis
Posten sporing	Posten	(ikke klart)	gratis
NRK Radio	NRK	NRK(usikkert)	gratis
Gjensidige	Gjensidige	Making waves	gratis
Norsk Tipping	Norsk Tipping	Agens(usikkert)	gratis
TaxiNå!	Apphuset	Apphuset	betal
7-Eleven Norge	7-Eleven Norge	Apphuset	gratis
Holmenkollen Ski-Jumpt	Norsk Tipping	Norsk Tipping/Agens(usikkert)	gratis
Visit Norway	visit norway	Making waves	gratis
Norsk TV-guide	apps for en bedre verden	app for en bedre verden	gratis
Norsk Radio	apps for en bedre verden	apps for en bedre verden	gratis
Flyplass Pro	Frank Burmo	Frank Burmo	betal

Vedlegg 2: Utenlandske Android-applikasjoner gjennomgått i rapporten

Applikasjoner Android	Om tjenesten		
Utenlandske	Ansvarlig	Utvikler	
Spotify	spotify ltd	spotify ltd	gratis
Shazam	Shazam	Shazam	gratis
Fruit Ninja	Halfbrick Studios	Halfbrick Studios	betal
Chess Online	Cloudroid	Cloudroid	gratis
Barcodescanner	Zxing Team	Zxing Team	gratis
Evernote	Evernote corp	Evernote corp	gratis
Fingerprintsscanner	ComputerTime Co	ComputerTime Co	betal
Twitter	Twitter	Twitter	gratis
WhatsApp Messenger	WhatsApp Inc	WhatsApp Inc	gratis
Skype	Skype	Skype	gratis
Google Maps	Google	Google	gratis
Doodle Jump	Game House	Game House	betal
SoundHound	SoundHound	SoundHound	betal
TripAdvisor	TripAdvisor	TripAdvisor?	gratis
Vignette	Neilandtheresa	Neilandtheresa	betal
FatBooth	PiVi & CO	PiVi & CO	gratis
Facebook	Facebook	Facebook	gratis
Angry Birds	Rovio Mobile	Rovio Mobile	gratis
Springpad	Spring Partners	Spring Partners	gratis
Tiny Flashlight	Niolay Ananiev	Niolay Ananiev	gratis

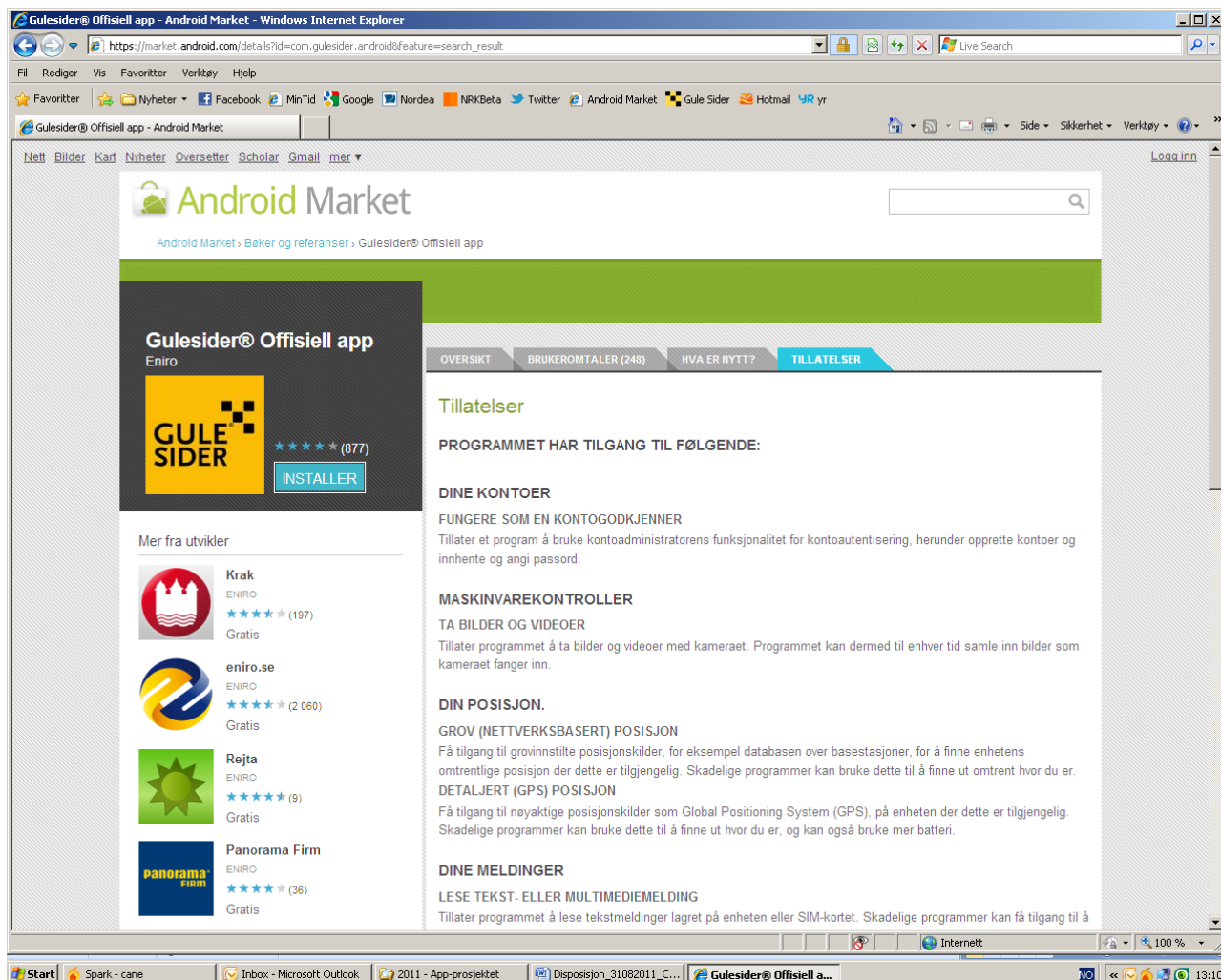
Vedlegg 3: Liste med spørsmål sendt til norske app-utviklere

Målsetningen med møtet er å få større innsikt i hvordan applikasjoner krever tilgang til personopplysninger lagret på telefonen, som f.eks lokasjonsdata, data fra kontaktlisten, kalenderen, bilder og lyd, nettleserhistorikk, ringehistorikk, nedlastede filer og telefon-id. Spørsmål vi ønsker å diskutere er:

- Hvordan reflekterer deres virksomhet rundt denne problemstillingen?
- Er det mulig å lage tjenester som har god funksjonalitet men som samtidig er personvernvennlige?
- Er det f.eks mulig å utvikle apper hvor forbrukeren selv kan ”skalere” hvilke opplysninger appen skal få tilgang til (selv bestemme grad av funksjonalitet i appen – med/uten tilgang til lokasjon, med/uten tilgang til kontaktliste)?
- Hvordan benyttes de innsamlede opplysningene fra app-brukerne? Hvilken tilgang til brukeropplysninger får oppdragsgiver og hva slags opplysninger kan app-utvikler få tilgang til? Selges eller formidles opplysningene på annen måte videre til tredjepart?
- Hvorfor kommer så få apper med en personvernpolicy?
- Er det forskjeller mellom plattformene når det gjelder i hvor stor utstrekning appene krever tilgang til personopplysninger på telefonen?
- Ev andre personvernmessige sider ved mobilapplikasjoner som kommer frem under samtalen.

Vedlegg 4: Eksempel fra informasjonsside i Android Market

Eksempel på liste over opplysninger som det opplyses om at Android-appene krever tilgang til.



Vedlegg 5: Oversikt over samtlige informasjonselement appene krever tilgang til

[illegible]

Vedlegg 6: Gjennomgang av norske apper med personvernerklæring

	Tilstrekkelig personvernerklæring for appen
Norske	
DNB Nor eiendom	Nei
Nordea	Nei
Fokus Mobilbank	Nei
Gulesider	Nei
Matprat	Nei
YR.no Widget	Nei
Wimp	Nei
Trafikanten offisiell	Litt informasjon
TV 2 Sporten	Nei
Posten sporing	Nei
NRK Radio	Nei
Gjensidige	Nei
Norsk Tipping	Nei
TaxiNå!	Nei
7-Eleven Norge	Nei
Holmenkollen Ski-Jumpt	Nei
Visit Norway	Nei
Norsk TV-guide	Nei
Norsk Radio	Nei
Flyplass Pro	Nei