



APPENES INFORMASJON OM TILGANG TIL PERSONOPPLYSNINGER

En kartlegging, oktober 2014

Sammendrag

I mai 2014 sjekket eller sveipet, Datatilsynet apper for mobiltelefoner og nettbrett sammen med 25 andre personvernmyndigheter i GPEN Privacy Sweep. GPEN står for Global Privacy Enforcement Network, og er et nettverk av personvernmyndigheter. Målet med årets sveip var å kartlegge hvilken informasjon som finnes om appers bruk av personopplysninger, enten i appbutikken eller i selve appen. Vi så spesielt på informasjon om appenes bruk av forskjellige tilganger til informasjon fra smarttelefonen eller nettbrettet, for eksempel lokasjonsdata, kontaktlister, mikrofon eller kamera.

Informasjon om hvordan appen bruker tilgangene den ber om, og hvorfor appen trenger disse tilgangene er viktig for de som vurderer å ta appen i bruk. Sveipet viser at det er svært varierende om virksomhetene bak appene informerer tilfredsstillende om dette. Vi har funnet alt fra apper som gir utdypende og spesifikk informasjon om hvordan de bruker tilganger, til apper som gir dårlig eller ingen informasjon om dette.

Gjennomføringen av sveipet

Datatilsynet sveipet 72 apper i løpet av en dag. Utvalget bestod av populære norske apper og store, kjente apper fra andre land. Blant de 72 appene vi sjekket, er det en svak overvekt av norske apper. En norsk app vil si at den som står som ansvarlig for appen i appbutikken er norsk. De 26 landene i GPEN-sveipet har til sammen sjekket over 1200 apper.

Innholdet i rapporten og hovedfunn

Rapporten handler primært om resultatene fra den norske delen av GPEN-sveipet. Den viser samtidig noen tall fra de samlede internasjonale resultatene. I tillegg sammenligner vi våre funn med to konklusjoner fra rapporten «Hva vet appen om deg?» som vi skrev i 2011.

Mange apper lenker til en personvernerklæring i appbutikken, og vi finner også en del personvernerklæringer på nettsidene til virksomhetene som er ansvarlig for appene. Et sentralt spørsmål i sveipet er om personvernerklæringene beskriver appens bruk av personopplysninger, ikke bare den ansvarlige virksomhetens generelle bruk av personopplysninger. Kun for 38 prosent av appene som hadde en personvernerklæring, konkluderte vi med at erklæringen beskrev appens bruk av personopplysninger.

I mange tilfeller får brukerne en del relevant informasjon, men at informasjonen ikke nok til at brukeren kan ta stilling til appens behandling av personopplysninger. Bare

omtrent to av fem apper forklarte hvordan de samler inn, bruker og eventuelt deler personopplysninger for alle tilgangene de ber om.

Rapportens mest urovekkende funn er at 31 prosent av appene ber om tilgang til opplysninger de som gjennomførte sveipet ikke forstår at appen trenger for å utføre sin funksjon. Resultatet er det samme i de samlede GPEN-tallene.

Innhold

Sammendrag	2
1. Personvern og apper.....	4
2. Om appsveipet.....	5
Et internasjonalt prosjekt GEPN	5
Gjennomføringen av det norske sveipet.....	5
Forhold leseren bør være oppmerksom på	5
3. Tall om appenes tilganger	7
De fleste apper ber om flere tilganger	7
Hvor mange tilganger ber hver app om.....	7
Din posisjon er mest etterspurt	8
4. Appens informasjon om personvern	9
Svært varierende informasjonen om personvern i appene	9
Det skal være lett for brukerne å finne informasjon om den enkelte app	10
Hvor god er appens informasjon om behov og begrunnelse for tilganger?	12
Tilganger brukeren ikke forstår at appen skal ha	14
Hva har skjedd siden vår apprapport i 2011?	15
5. Oppsummering.....	16
Hva skal til for å bedre situasjonen?	16
Vedlegg 1 - sveipeskjema	17
Vedlegg 2 - appene i det norske sveipet	20
Vedlegg 3 - oversikt over deltagere i sveipet.....	23

1. Personvern og apper

Bruken av smarttelefoner og nettbrett har økt kraftig de siste årene, og er i dag en viktig del av nordmenns hverdagsliv. I 2013 hadde hele 73 prosent av nordmenn mellom 9 og 79 år tilgang til en smarttelefon og 61 prosent hadde tilgang til et nettbrett¹. I 2013 ble det solgt i underkant av en million nettbrett i Norge, som nesten er en dobling fra året før².

Sammen med smarttelefoner og nettbrett har mengden apper eksplodert. I mai 2013 annonserte Apple at de hadde nådd 50 milliarder nedlastinger til iOS-universet, mens kunne Google kunne annonsere at de hadde 48 milliarder nedlastinger til Android-enheter³.

Smarttelefoner og nettbrett er svært nær oss i det daglige. Enhetene kan blant annet vite hvor vi er gjennom posisjonering. Den vet hvem vi har kontakt med og ofte også innholdet i kommunikasjonen vår. Vi bruker den til å lagre minner gjennom bilder og den kan gjennom ulike sensorer registrere hva vi driver med til enhver tid. Apper kan potensielt få tilgang til all denne informasjonen, bruke den og sende den videre uten at vi vet om det eller har kontroll over hvem som får informasjonen.

Dette er grunnen til at personvern er et viktig tema i denne sammenhengen. God informasjon om hvilke tilganger appene har og hvordan disse tilgangene brukes, er nødvendig for å sikre godt personvern. Ikke fordi vi skal si nei til gode tjenester, men fordi brukerne skal være i stand til å bestemme over egne personopplysninger.

Appbrukerne har behov for informasjon og virksomhetene har behov for tillit

Informasjon er ett av de mest fundamentale elementene i et godt personvern. Den opplysningene gjelder skal få informasjon om hvordan hans eller hennes personopplysninger blir samlet inn og brukt. Prinsippet om informasjon og åpenhet er ikke bare viktig i seg selv. Det står også i sammenheng med et annet viktig personvernprinsipp, nemlig retten til å kunne velge selv. Kombinasjonen av informasjon og valg er sentralt for apper og personvern. Ut fra informasjon du får om hvordan appen samler inn og bruker personopplysningene

dine, er det opp til deg å velge om du ønsker å laste med appen eller la det være.

Når du gir en app tilgang åpnes det dører. Du gir ikke bare tilgang til den spesifikke operasjonen appen trenger å gjøre, du gir den også tilgang til noe større. Å gi tilgang til ulike deler av smarttelefonen eller nettbrettet ditt kan sammenliknes med å gi noen tilgang til forskjellige rom i huset ditt. Grunnen til å gi for eksempel en håndverker tilgang til ett eller flere rom, kan være å få en jobb gjort. Selve jobben kan være liten, men når du har gitt vedkommende tilgang er hele rommet og alt som er der inne tilgjengelig for den som har tilgang. Det er nesten ikke mulig å verifisere hvordan tilgangen til rommene faktisk brukes. Dette er dilemmaet appbrukeren møter når en app ber om ulike tilganger. Appen må gi god informasjon om sin faktiske bruk av tilgangene og brukeren må ha tillit både til denne informasjon og til den eller de som er ansvarlig for appen.

De som tilbyr apper er avhengig av appbrukernes tillit. Det er en klar sammenheng mellom åpenhet og tillit. Sannferdig og klar informasjon og at bruken av personopplysninger fremstår som relevant og rimelig for tjenesten appen tilbyr, er viktige kriterier for å få appbrukerens tillit eller ikke.

¹ <http://www.medienorge.uib.no/statistikk/medium/ikt/388>

² <http://www.medienorge.uib.no/statistikk/medium/ikt/389>

³ <http://www.nrk.no/livsstil/nordmenn-er-ville-etter-nettbrett-1.11517699>

⁴ <http://www.elektronikkbransjen.no/Presse/Pressemeldinger/Nordmenn-kjoeper-stoerre-TV-og-flere-nettbrett>

⁵ <http://www.digi.no/917491/android-raser-forbi-ios>

2. Om appsveipet

Et internasjonalt prosjekt: GPEN Privacy Sweep

Det norske appsveipet er del av det internasjonale prosjektet "GPEN Privacy sweep". GPEN står for Global Privacy Enforcement Network, og er et internasjonalt nettverk av personvernmyndigheter. GPEN gjennomførte et personvernsveip for første gang i 2013 og har som mål at dette skal være en årlig aktivitet. Antallet deltagere har steget fra 18 personvernmyndigheter i fjor til 26 i år. Datatilsynet var også med på fjorårets sveip. Da sjekket vi om virksomheter hadde personvernerklæringer på sine nettsider.

Sveipet fant sted mellom 12. og 16. mai 2014. De 26 deltakende personvernmyndighetene gikk gjennom til sammen 1211 apper. Alle testet det samme slik at det skal være mulig å få et samlet resultat for hele sveipet. Dette er på ingen måte noen dyptgående sjekk av hver app. Sveipet handler om å få oversikt over et sett forhåndsdefinerte vurderingspunkter. For hver app fyller sveiperne ut et relativt omfattende skjema.

Årets appsveip handler om brukernes mulighet til å finne informasjon om appens bruk av personopplysninger og hvor god denne informasjonen er. Fokus er hvilken informasjon om personvern brukeren får for hver av tilgangene de ulike appene ber om.

Personvernmyndighetene som deltar bestemmer selv hvor store ressurser de vil bruke på sveipet. Sveipeskjema og metodikk gir visse rammer, men deltagerne velger selv hvilke apper de vil sveipe og om de for eksempel kun ville se på apper fra eget land, mye brukte apper eller andre typer apper. Det er også mulig å velge ut en spesiell type apper, for eksempel helse-apper. Hvilket utstyr som brukes i testen, smarttelefoner eller nettbrett og plattform (iOS og Android) som sjekkes er opp til deltakerlandene.

Etter sveipet har deltakerlandene diskutert funn og trender. Vi står samlet i ønsket om å formidle funnene våre for å bevisstgjøre forbrukere, apputviklere og appeiere om temaet apper og personvern.

Datatilsynet har valgt å skrive en rapport om våre funn. Vi mener situasjonen er langt fra så god som den burde være. En stor andel av appene vi har sjekket, informerer ikke brukerne sine godt nok. Dette funnet tar vi med oss i vårt videre arbeid og vi vil være spesielt opptatt av å formidle dette til apputviklere og virksomheter som ønsker å ta i bruk apper.

Vi mener at rapporten også er nyttig for brukere eller andre som er interessert i apper. Å sikre godt personvern i apper avhenger ikke bare av flinke utviklere og appeiere, men også bevisste forbrukere som er kritiske til hvilke apper de velger og stiller krav til de som er ansvarlige for appen.

Gjennomføringen av det norske sveipet

Det norske sveipet ble utført av sju ansatte i Datatilsynet 12. mai 2014.

Vi sjekket både utenlandske og norske apper. En norsk app vil si at virksomheten som er oppgitt som ansvarlig i appbutikken er norsk. Utvalget vårt bestod av 84 apper som enten var populære norske apper eller store, kjente apper fra andre land. Av ulike grunner fikk vi ikke fullstendige data om 12 av disse, for eksempel fordi noen av dem krevde at man registrerte seg med navn eller fødselsnummer. Dette hadde vi på forhånd bestemt oss for å ikke gjøre. Vi har derfor ikke tatt med disse appene i resultatene våre.

Dataene i det norske sveipet består derfor av 72 apper, hvorav 54 prosent er norske og 46 prosent er utenlandske. Blant disse er det flest gratis-apper, men også noen apper brukerne må betale for å laste ned. Vi brukte kun smarttelefoner. Tre av sveiperne brukte Android som plattform og fire brukte iOS som plattform.

Sveipeskjemaet og listen over apper vi sjekket ligger som vedlegg til rapporten.

Forhold leseren bør være oppmerksom på

Utvalget er ikke representativt. Gjennom vårt utvalg av apper, har vi forsøkt å beskrive forholdene for en norsk appbruker. Resultatene fra det norske sveipet må derfor ikke forstås som representative, verken for norske apper generelt eller for apper som er mye brukt av nordmenn. Til det er antallet apper som er sjekket for lavt, og det ligger også utvelgelseskriterier til grunn som kunne vært annerledes. Antallet norske apper og det at de ulike deltakerlandene har brukt forskjellige utvelgelseskriterier gjør at vi ikke kan si noe sikkert om forholdet mellom norske apper og apper fra andre land (for eksempel ved å sammenlikne de norske appene med tallene for det samlede GPEN-sveipet). Vi mener likevel at tallene gir et godt overblikk over situasjonen for norske appbrukere.

Kun en rask sjekk av hver app. Sveipet legger opp til en rask sjekk. Dette betyr at vi kan ha oversett enkelte forhold ved noen apper. Delvis på grunn av dette, har vi valgt å ikke publisere resultatene for hver app. Å gjøre en vurdering av hver enkelt app er heller ikke formålet med rapporten. Den skal gi et overordnet bilde av situasjonen.

At sjekken er relativt rask, kan ha gitt noe underrapportering av tilganger for iOS-apper. For Android-appene listes alle tilganger opp før nedlasting. Det som gjorde det enkelt for sveiperne å få oversikt over alle tilgangene appen ber om. For iOS-appene kommer derimot tilgangsforespørslene underveis, gjerne knyttet til bruken av appene. Fordi vi brukte kort tid på hver av app, er det mulig at ikke vi ikke har utløst alle relevante tilgangsforespørsler for iOS-appene.

Skjemaet gir et visst rom for tolkning. Enkelte spørsmål i skjemaet gir et rom for tolkning. Det gjelder både hvordan spørsmålet forstås, og hvor grensen skal gå for et «ja» eller et «nei». I Datatilsynet hadde vi før sveipet diskutert oss frem til en felles linje. Vi kan likevel ikke utelukke at det er mindre tolkingsforskjeller mellom de forskjellige landes sveip. I rapporten utdyper vi ved et par anledninger hvordan vi har vurdert spørsmålet.

Tilganger telles på et kategorinivå. Tilgangene appene ber om er talt på et kategorinivå, delt i ti forskjellige kategorier i sveipeskjemaet. For noen tilganger kan antallet, rent teknisk, egentlig være noe mer komplisert. For eksempel er lokasjon én kategori i sveipet, men kan bety at appen ber om flere forskjellige tilganger knyttet til lokasjon som grov lokalisering eller detaljert lokalisering ved hjelp av GPS.

3. Tall om appenes tilganger

Dette kapitlet beskriver hvor mange tilganger appene bad om, uavhengig av hvor god informasjonen om personvern var. Dette er en viktig introduksjon til neste kapittel, som ser på appenes evne til å gi god informasjon om personvern for de tilgangene de ber om.

I sveipet deles tilgangene opp slik: Lokasjon, kontakter, kalender, mikrofon, kamera, enhetsidentifikator (IMEI, tlf.nr, serienummer), tilgang til andre kontoer, SMS, telefonlogg og annet.

De fleste apper ber om flere tilganger

Sveipet viser tydelig at det er flere apper som ber om tilganger enn apper som ikke ber om tilganger.

I det norske sveipet ba 68 prosent eller omtrent to tredjedeler av appene om én eller flere tilganger. Hvis vi kun ser på de norske appene i vårt sveip, er forholdet likt. To tredjedeler ber om tilganger, mens en tredjedel ikke ber om noen tilganger.

Tallet fra det samlede internasjonale sveipet viser at en noe høyere andel apper som ber om tilganger. Tre fjerdedeler eller 75 prosent ber om minst én tilgang, mens en fjerdedel ikke ber om noen tilganger.

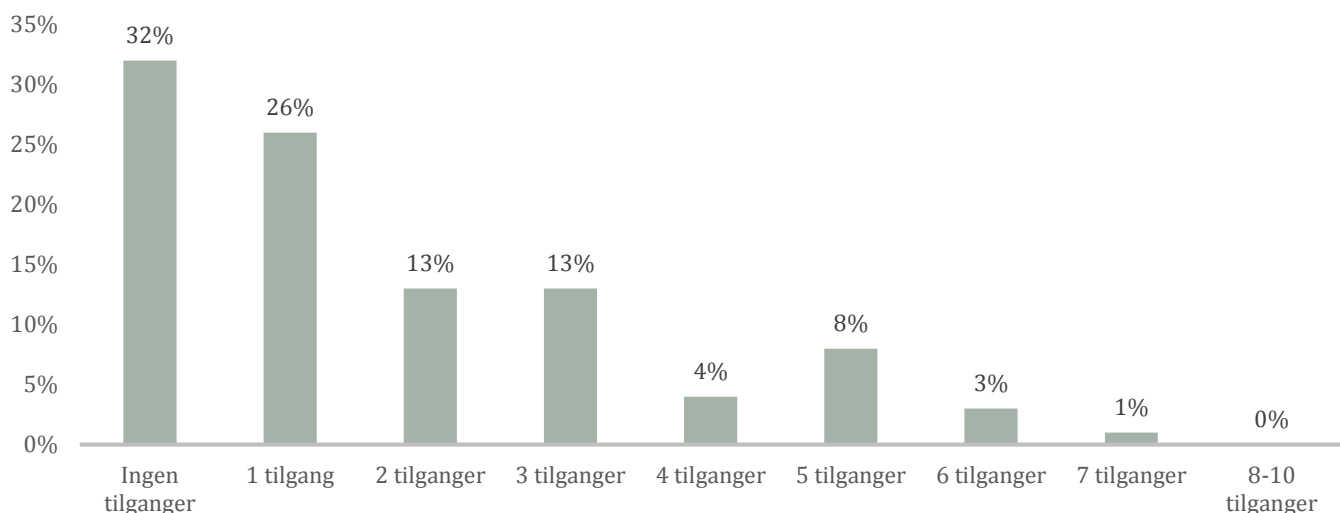
Hvor mange tilganger ber hver app om?

I det norske sveipet ber hver app om gjennomsnittlig 1,7 tilganger. Dersom en ser bort fra appene som ikke ber om noen tilganger, ligger gjennomsnittet på 2,6 tilganger per app.

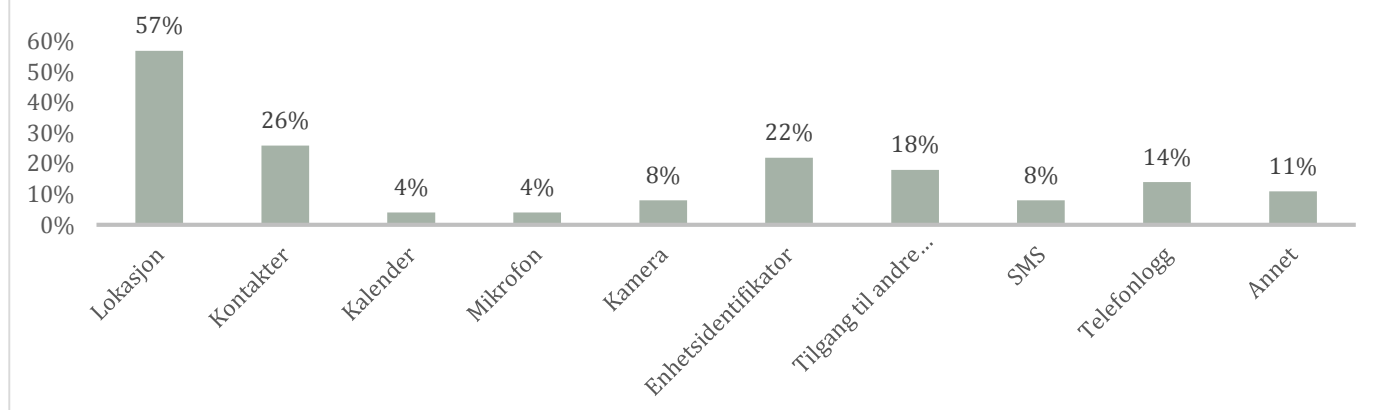
Diagrammet viser fordelingen av apper etter hvor mange tilganger de ber om. Tallene er fra det norske sveipet. Grafen viser at de fleste apper ikke ber om noen tilganger.

For appene som ber om tilganger, ber de fleste om en, to eller tre tilganger. Totalt er det 16 prosent av appene som ber om fire eller flere tilganger. Det høyeste antallet tilganger en app bad om i vårt utvalg var sju, og det fant vi kun i én app.

APPER FORDELT ETTER ANTALL TILGANGER DE BER OM



ANDEL APPER SOM BER OM ULIKE TILGANGER



Din posisjon er mest etterspurt

Den klart mest etterspurte tilgangen er «lokasjon», det vil si hvor du befinner deg. Over halvparten, 57 prosent, i det norske sveipet, ber om tilgang til lokasjon. Avgrenset til kun norske apper gir det tilnærmet samme prosentandel. De nest mest etterspurte tilgangene er «kontakter» og «enhetsidentifikator» på henholdsvis 26 og 22 prosent. De minst etterspurte tilgangene er «mikrofon» og «kalender», begge på fire prosent.

Figuren nedenfor viser andelen av alle appene i det norske sveipet som ba om ulike tilganger. Også i de internasjonale tallene er «lokasjon» den meste etterspurte tilgangen. Deretter følger «enhetsidentifikator» og «tilgang til andre kontoer». Minst etterspurt er «kalender» og «SMS».

4. Appenes informasjon om personvern

Det sentrale spørsmålet i sveipet var hvilken informasjon om personvern brukerne får ved nedlasting av apper i appbutikken. I dette kapittelet beskriver vi våre funn om dette sammen med våre kvalitative vurderinger av informasjonen.

Vi har valgt å avgrense funnene til fem temaer som vi synes er særlig viktige for å illustrere hvilken informasjon om personvern en appbruker får.

Svært varierende informasjonen om personvern i appene
"Svært varierende" er på flere måter en riktig beskrivelse av appenes informasjon om personvern. Det er ikke bare om det finnes personverninformasjon som varierer, men også om informasjon som gis gir gode svar. Det varierer også om tilgangene den enkelte app ber om fremstår som forståelige ut fra tjenesten appen gir.

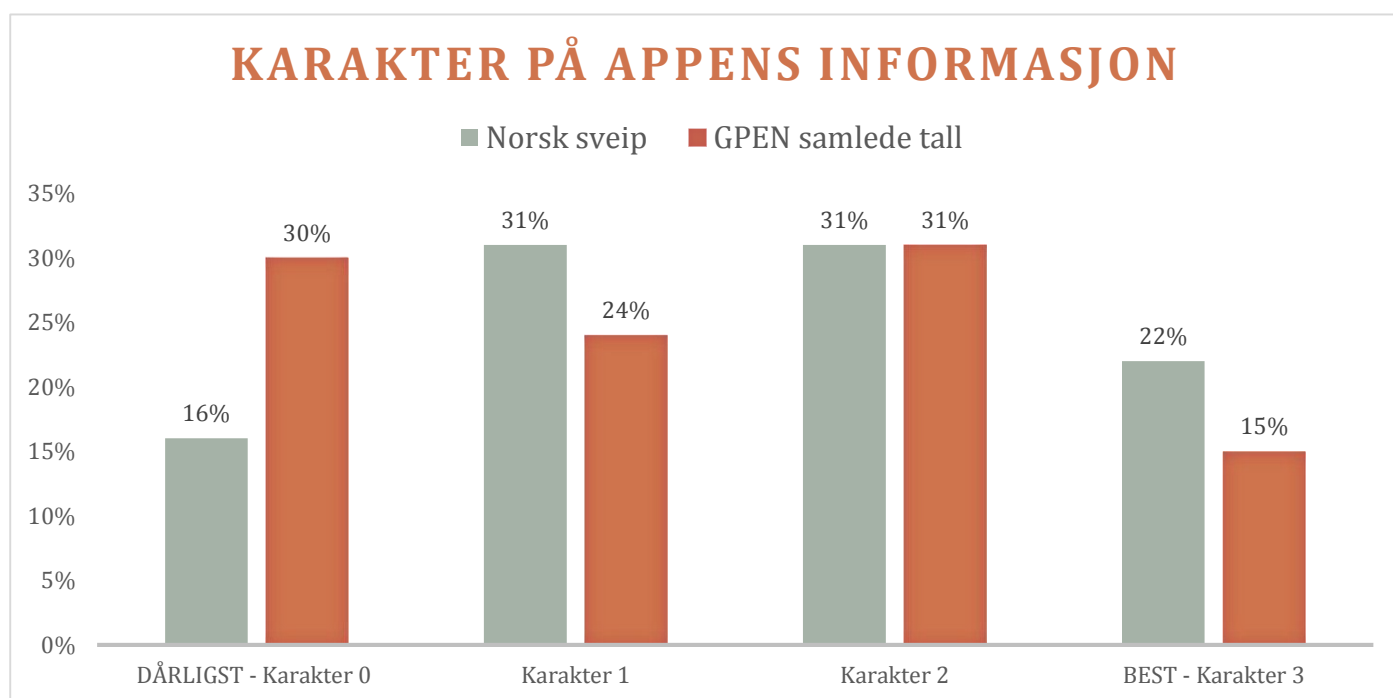
Hver app fikk en karakter ut fra en helhetsvurdering av hvor god informasjonen om personvern den ga. Her så vi

på den samlede, tilgjengelige informasjonen i appbutikken og eventuelt personvernerklæringen. Resultatet viser at det er svært varierende hvor god informasjonen er.

Diagrammet viser tallene fra det norske sveipet og de samlede internasjonale resultatene. Karakteren 3 er best, og 0 er dårligst. Apper som ikke ba om noen tilganger er utelatt fra disse tallene⁴.

Appene i sveipet er fordelt over hele karakterskalaen og alle karakterer har en betydelig prosentandel. Det er noen forskjeller mellom resultatet fra det norske sveipet og de internasjonale tallene, men resultatene viser samme hovedpoeng. Kvaliteten på informasjonen appbrukeren får varierer mye og er i sum for dårlig. Rundt halvparten av appene får en av de to dårligste karakterene.

Samtidig viser både de internasjonale og de norske resultatene at en del apper gir god informasjon og får derfor toppkarakter. Samlet sett er denne andel likevel liten. Vi ser også mange eksempler på at det gis dårlig eller ingen informasjon. At det er så stor spredning i appenes informasjon om personvern for den enkelte tilgang er et



⁴ Apper som ikke ba om tilganger fikk "karakteren" ("not applicable"). I europeisk personvernlovgivning er kravet til informasjon om personvern knyttet til at det skjer en behandling av personopplysninger. Man må derfor ikke informere når det ikke skjer noen behandling av personopplysninger. Når det gjelder apper, vil

det likevel ofte være en fordel om det finnes informasjon om at appen ikke krever tilganger eller bruker personopplysninger.

viktig funn. De fleste apper har noe informasjon om personvern for hver tilgang, men denne informasjonen er ofte ikke god nok til at brukerne kan ta en informert beslutning om hva det å laste ned appen kan bety for deres personvern.

At det er så varierende hvor mye informasjon apper gir om personvern gir ulike utfordringer. En vanlig appbruker kan finne alt eller ingenting som resultat når han eller hun søker informasjon om dette. Dette er uheldig fordi det kan føre til at brukerne ikke tar seg bryet med å se etter slik informasjon før de laster ned en app.

Det skal være lett for brukerne å finne informasjon om den enkelte appen

Informasjon som er tilgjengelig ved nedlasting av en app, må gjøre det tydelig for brukeren hva som gjelder for appen. I tillegg må brukeren lett kunne finne frem til og forstå informasjonen. Hvis ikke er det stor sjanse for at informasjonen som er tilgjengelig kun er nyttig for de brukerne som er spesielt interesserte i dem.

Et viktig funn i sveipet er at selv om vi ofte finner informasjon om personvern generelt, gir ikke tekstene god nok informasjon om personvern i appen.

For appene i det norske sveipet fant vi i de fleste tilfeller en personvernerklæring når appene bad om tilganger. Denne var tilgjengelig enten direkte fra appbutikken eller på virksomhetens nettsider. For appene som ikke ber om tilganger er det stikk motsatt. Vi finner som hovedregel ikke noen personvernerklæringer for disse appene.

Sett fra et personvernståsted, er det ikke tilfredsstillende at apper som ber om tilganger ikke har en personvernerklæring. Samtidig er det mest skuffende hvor lite informasjon noen av erklæringene gir. I en personvernerklæringen har virksomheten en mulighet til å kunne gi god informasjon om sin bruk av personopplysninger. I de fleste tilfeller beskriver

personvernerklæringene likevel ikke helt konkret hvordan den aktuelle appen bruker personopplysninger. Selv om vi finner en personvernerklæring, er det altså på ingen måte sikkert at appbrukeren har noe særlig nytte av den.



Karakterene er gitt etter denne skalaen:

Karakter 0 = Ingen info om personvern, utover tilganger.

Karakter 1 = Informasjonen om personvern som brukeren får når tilgang gis, er ikke tilfredsstillende; sveiperen vet ikke hvordan personopplysninger blir samlet/brukt/delt.

Karakter 2 = Informasjonen om personvern som brukeren får når tilgang gis, beskriver i noen grad appens innsamling/bruk/deling av personopplysninger, men sveiperen er fremdeles usikker på hvorfor appen trenger noen av tilgangene.

Karakter 3 = Informasjonen om personvern som brukeren får når tilgang gis, forklarer tydelig hvordan appen samler/bruker/deler personopplysninger. Sveiperen er informert om appens bruk av personopplysninger.

Sveipeskjemaet hadde følgende spørsmål: «Beskriver personvernerklæringen appens bruk av personopplysninger (ikke bare behandlingsansvarliges generelle bruk av personopplysninger)?» For bare 38 prosent av appene hvor vi fant en personvernerklæring var svaret «ja»⁵. Det er med andre ord langt under halvparten av personvernerklæringene som faktisk gir informasjon om den aktuelle appen.

De samlede GPEN-tallene er bekymringsverdige på dette feltet. Derfor er dette ett av de mest sentrale funnene i sveipet. Tallene fra det norske sveipet er enda dårligere⁶. Vi mener dette viser et svakt punkt i virksomhetenes kommunikasjon om personvern. Altfor få virksomheter informerer spesifikt om appens bruk av personopplysninger.

⁵ Det var ikke krav om at det måtte være en egen personvernerklæring for at sveiperen kunne svare «ja», men at det må være relativt lett for leseren å finne spesifikk informasjon om den aktuelle appens bruk av personopplysninger.

⁶ De samlede GPEN-tallene tar utgangspunkt i alle apper, uavhengig av om de ber om tilganger eller ikke. For 41 % av appene svarte sveiperne «ja» på spørsmålet «Beskriver personvernerklæringen appens bruk av personopplysninger (ikke bare behandlingsansvarliges generelle bruk av personopplysninger)?» Det

tilsvarende tallet for det norske sveipet er 24 prosent. Med basis i små tall i det norske sveipet, ulikt utvalg av apper i ulike land og muligheten for at deltakerlandene har forstått spørsmålet litt forskjellig, må vi være forsiktige med sammenlikninger. Vi vil likevel nevne at det er en høyere andel apper som ikke ber om tilganger i den norske sveipet sammenliknet med det GPEN-tallene. Siden disse appene har lite informasjon om personvern, trekkes resultatet noe ned for det norske sveipet. Det kan likevel ikke forklare forskjellen mellom det norske sveipet og de samlede GPEN-tallene.

Diagrammet nedenfor viser hvor liten andel av appene som hadde en personvernerklæring med informasjon om appens bruk av personopplysninger.

Resultatet er nedslående og viser et stort forbedringspotensial.

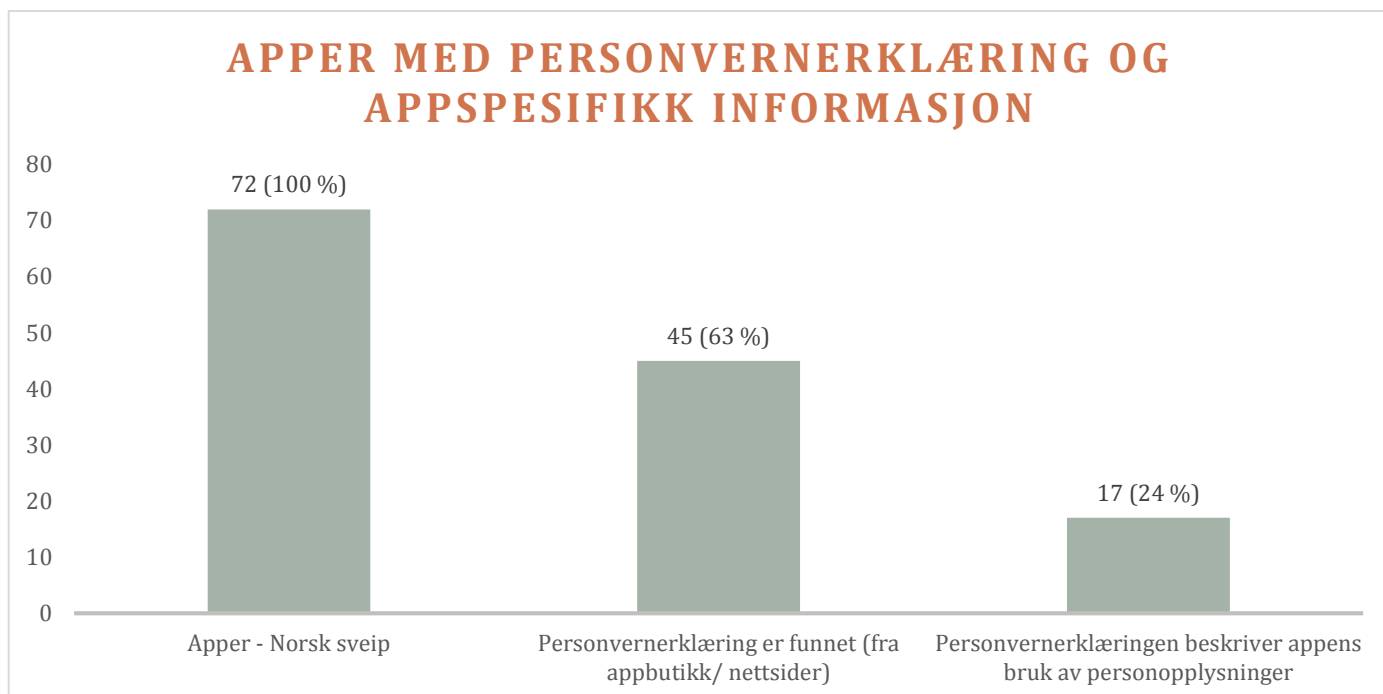
Spesifikk informasjon om appenes bruk av personopplysninger er viktig. I mange tilfeller ligger det, som en del av oversiktsinformasjon om appen i App Store eller Google Play en peker til «personvernregler» eller liknende. Under sveipet så vi mange eksempler på at disse pekerne viser til personvernerklæringer som beskriver apputvikleren eller appeieren sin generelle håndtering av personopplysninger. Personvernerklæringene som informerer om virksomhetens totale bruk av personopplysninger i et bredt spekter av tjenester er ofte svært lange. I andre tilfeller finner vi erklæringer som kun informerer om hvordan virksomhetens internettside samler inn personopplysninger, for eksempel bruken av informasjonskapsler. Disse er trolig laget primært for brukere av nettsiden, ikke appen.

En henvisning til lange og omfattende personvernerklæringer om virksomhetenes totale bruk av personopplysninger kan representere et problem for appbrukeren. Når han eller hun klikker på en personvernerklæring for å finne informasjon om appen, blir det unødig komplisert og ofte umulig å finne denne

informasjonen. Dette kan skape usikkerhet om, og gi grobunn for misforståelse om hva appen gjør. Selv om informasjonen i erklæringen er god, rent innholdsmessig, blir det likevel for tidkrevende for brukeren å finne ut hvilken informasjon som er relevant for appen.

Vi vil gjerne understreke følgende. Lange personvernerklæringer om virksomhetenes generelle bruk av personopplysninger er ikke nødvendigvis et problem. Dersom erklæringen har en oversiktlig struktur og en innholdsfortegnelse slik at appbrukeren lett kan finne informasjon om appen, kan den fungere godt. Noen virksomheter bygger opp sine personvernerklæringer med en tematisk oversikt med pekere til hver artikkel i erklæringen. Det fungerer ofte godt. En annen løsning er at appen har en helt egen personvernerklæring. Det siste vil nok uansett være det enkleste for appbrukeren.

Datatilsynet har ved gjentatte anledninger anbefalt at virksomheter har en personvernerklæring på sine nettsider som informerer om virksomhetens bruk av personopplysninger. Spørsmålet er om en slik erklæring er egnet som primærkilden for informasjon til brukere som skal laste ned en konkret app.

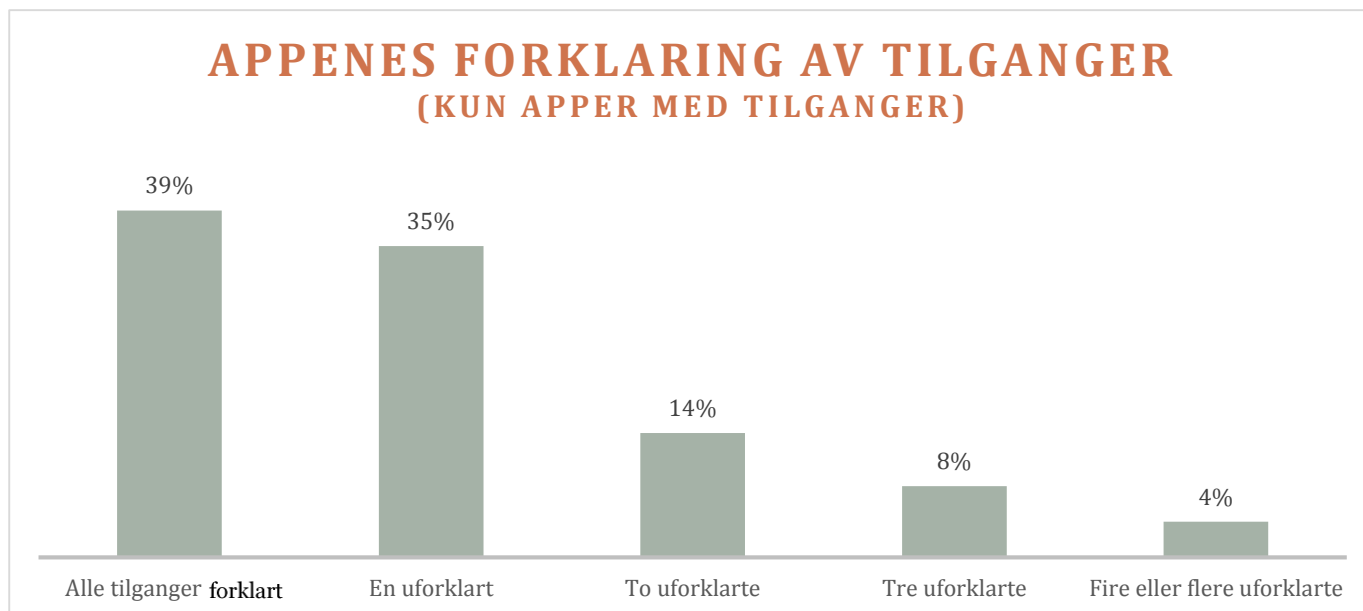


Hvor god er appens informasjon om behov og begrunnelse for tilganger?

Informasjon om hvordan appen bruker tilgangene den ber om, og hvorfor appen trenger disse tilgangene er viktig for at brukerne skal kunne ha oversikt. I sveipet fant vi gode eksempler på slik informasjon som gav en tydelig og god forklaring. Likevel er det mange apper som ikke møter brukernes informasjonsbehov på en god nok måte.

Skjemaet vi brukte i sveipet hadde følgende spørsmål: «Forklarer appen hvordan den samler, bruker og deler personopplysninger i forbindelse med tilgangen?» Vi noterte den tilgjengelige informasjonen og forklarte hver enkelt av tilgangene appen bad om med henblikk på de tre aspektene «samler», «bruker» og «deler»⁷. Dette gav oss en god indikator på hvor dekkende og konkret appen informerte om selve bruken av personopplysningene. Diagrammet viser resultatene.

Diagrammet viser apper fordelt etter antallet tilganger appen ber om som ikke er forklart for brukeren. Vi har kun tatt med apper som ber om tilganger. Disse appene bad om gjennomsnittlig 2,6 tilganger hver.



⁷ Den enkelte sveiper svarte «ja» eller «nei» på dette spørsmålet ut fra en skjønnsmessig vurdering. Det betyr at vi har svart «ja» også i tilfeller hvor tilgangen er temmelig bra beskrevet, men hvor vi mener forklaringen ikke dekker alle de tre aspektene «samler», «bruker» og «deler» godt nok. Spørsmålsformuleringen bidrar til å legge listen relativt høyt for at sveiperen kan svare «ja». Det vil for eksempel ikke være godt nok at innsamlingen alene er grundig beskrevet dersom vi ikke forstår hvordan opplysningene brukes og eventuelt deles.

Dette er et nedslående resultat. Kun godt under halvparten av appene, omtrent to av fem, forklarte alle sine tilganger med henblikk på innsamling, bruk og eventuell deling av personopplysninger. De resterende appene bad om én eller flere tilganger de ikke forklarte. De fleste appene i det norske sveipet bad om én eller flere tilganger de ikke forklarte, eller gav en mangelfull beskrivelse av hvorfor de trengte tilgangen eller hvordan den brukes.

Appens informasjon om personvern bør beskrive bruk og behov for hver enkelt tilgang, gjerne systematisk. NSB er et godt eksempel på en virksomhet som har gjort dette for sin app. I personvernerklæringen⁸ som beskriver appen finner vi et eksempel på en tilgang som det var viktig å forklare (se under). Eksempelet illustrerer et generelt poeng. Selve beskrivelsen av hva appen får tilgang til, som dine sms eller din kalender, kan fremstå som skremmende dersom du ikke får en forklaring på hva disse skal og ikke skal brukes til.

Vi synes NSBs løsning fungerer godt. Den forklarer hva appen bruker kalenderen til og derfor også hvorfor appen ber om tilgang til den. I tillegg avklarer teksten at det man kan frykte for eksempel at appen leser dine avtaler, ikke skjer.



Tekst hentet fra NSB sin personvernerklæring

Telefonens kalender

Når man har lastet ned billetten har vi gjort det enkelt å legge til reisen i kalenderen. Fra billetten kan man velge å lagre reisedetaljer til selvvalgt kalender slik at man kan få varsling og se når man skal ut og reise.

Før **Android** appen lastes ned blir bruker informert om blant følgende: "...lese kalenderaktiviteter og konfidensiell informasjon, legge til eller endre kalenderhendelser og sende e-post til gjester uten eiernes viten." Det er viktig å poengtere at appen ikke leser konfidensiell informasjon, ikke endrer på dine kalenderhendelser og ikke sender e-post uten at du vet om det. Det at appen beskriver slike mulige tilganger er forklaringer som Google har skrevet når NSB-appen bruker noen av Google sine API.



Appen til 180.no + Gratis er et annet godt eksempel på en app med en kort, men god beskrivelse av hvorfor en app ber om forskjellige tilganger og hva disse skal eller ikke skal brukes til. Appen beskriver sin bruk av tilganger i appbutikken, ikke i en personvernerklæring (se bildet av appen fra appstore). Legg særlig merke til informasjonen om hvorfor appen skal ha tilgang til brukernes meldinger.

Dette er to av flere eksempler på apper som gir god informasjon om hvilke tilganger den behøver og hvorfor. Dessverre er det langt mellom slike eksempler.

⁸ <https://www.nsb.no/om-nsb/behandling-og-bruk-av-personopplysninger>

Tilganger brukeren ikke forstår hvorfor appen skal ha

Selv der hvor det ikke finnes informasjon om hva en app skal bruke en tilgang til, kan det i mange tilfeller være selvforklarende for brukeren hvorfor appen må ha denne tilgangen. For eksempel er det logisk at en karttjeneste som skal hjelpe deg å finne veien fra der du er nå, må ha tilgang til hvor du befinner deg. I andre tilfeller er det vanskeligere eller umulig å forstå hvorfor en app har behov for en eller flere tilganger.

I sveipet så vi spesielt på om apper ber om tilganger brukeren trolig ikke forstår. Sveiperne svarte på følgende spørsmål: «I etterkant av sveipet, er tilgangen utenfor hva du ville forventet basert på appens funksjon?» Hva som er uventet eller uforståelig vil i dette tilfellet basere seg på sveiperens forståelse av appens tjeneste. Her vil vi presisere at sveiperen tok stilling til spørsmålet om forståelige eller ikke forståelige tilganger etter at vedkommende hadde lest personvernerklæringer og annen tilgjengelig informasjon om personvern. Resultatet viser dessverre at en stor del av appene vi sjekket bad om tilganger det var vanskelig å forstå hvorfor de skulle ha.

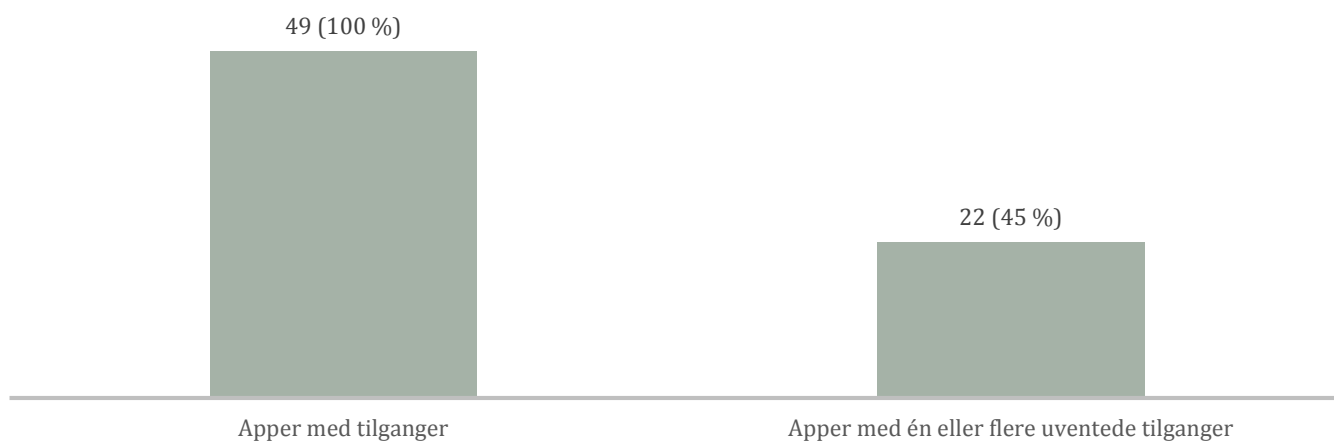
At en tilgang blir forstått som uventet, betyr ikke nødvendigvis at tilgangen ikke er relevant for tjenesten, eller at appen ikke trenger den. Vi tror at mange av tilgangene vi har kategorisert som uforståelige ville vært

forståelige for brukeren dersom appen forklarte hvorfor den ba om tilgangen. Samtidig har vi funnet eksempler på tilganger som er nevnt i personverninformasjonen, men som vi likevel mener er uventede eller uforståelige ut i fra appens funksjonalitet.⁹

Av de 49 appene i utvalget vårt som bad om ulike tilganger, var det 22 apper (45%) som bad om tilganger vi ikke forstod hvorfor de trengte. Slike uforståelige tilganger finnes i alle kategorier av tilganger unntatt «kalender». Fire av appene bad om tre tilganger vi ikke kunne forstå at de trengte, og en app bad om to uforståelige tilganger. De 17 resterende appene bad om en uforståelig tilgang hver. De fleste av tilgangene vi ikke forstår hvorfor appen skal ha, går inn i kategorien «lokasjon» (10 eksempler). Dette er som tidligere nevnt også den tilgangen flest apper ber om. Den nest mest vanlige kategorien av uforståelige tilganger er «tilgang til andre kontoer» (6 eksempler).

De 22 appene som bad om tilganger vi ikke forstod utgjør 31 prosent av alle appene i det norske sveipet. Da har vi tatt med både apper som bad om og som ikke bad om tilganger. Også i det samlede GPEN-sveipet bad 31 prosent av appene om tilganger som var uforståelige ut fra tjenestene de gir.

ANTALL APPER MED TILGANGER UTENFOR DET FORVENTEDE



⁹ Et eksempel på dette er en avis-app ber om tilgang til brukerens lokasjonsdata. Vi mener appens tjeneste er å levere nyheter og at hvor du befinner deg derfor ikke skal ha noen betydning for hva du får presentert av nyheter. Tilgangen er derfor kategorisert som utenfor det forventede. Lokasjonsdataene samles trolig inn for å fylle appselgers behov, nemlig inntektsmuligheter i form av reklame

basert på hvor du er. Om appen istedenfor generelle nyheter hadde presentert lokale nyheter etter hvor du befinner deg, ville vi forstått hvorfor den ber om tilgang lokasjonsdata.

Den store prosentandelen apper som ber om tilganger vi ikke forstår hvorfor de må ha, representerer ett av de mest alvorlige funnene i sveipet.

Hva har skjedd siden vår apprapport i 2011?

Vi mener det har skjedd en forbedring av hvordan apper informerer brukerne om personvern og sin bruk av personopplysninger sammenliknet med funnene fra vår rapport fra 2011¹⁰. For å illustrere hva som har endret seg og hva som ser likt ut som i 2011, sammenligner vi to konklusjoner fra 2011-rapporten med funnene fra årets norske appsveip.

En av konklusjonene fra 2011-rapporten var:

- 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.

I sveipet har en drøy halvpart, 56 prosent, en personvernerklæring tilgjengelig fra appbutikken, om vi avgrenser oss til de appene som ber om tilganger. Resultatet viser at det nå ganske ofte ligger informasjon eller en peker til informasjon om hvordan appen håndterer personopplysninger i selve appbutikken. Det betyr at det er naturlig å anta at appbrukere i dag har en bedre mulighet til å ta en kvalifisert beslutning om å installere en app eller ikke. Samtidig er det fortsatt stort rom for forbedring. Andelen informasjon som beskriver appens bruk av personopplysninger og ikke virksomhetens generelle bruk av personopplysninger er for lav. Informasjonen er også ofte mangelfull og det er for mange apper som ber om tilganger uten å forklare hvordan og hvorfor den trenger disse tilgangene.

En annen konklusjonene fra 2011-rapporten var:

- 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.

Inntrykket etter årets sveip er at konklusjonene fra 2011 stemmer i noen grad også med dagens situasjon selv om vi

ikke vil bruke ordet «sjeldent» om hvor ofte muligheten benyttes i dag. Vi fant 24 tilfeller hvor det var en personvernerklæring eller en lenke til en personvernerklæring, i appen. Det tilsvarer en tredjedel av de 72 appene i det norske sveipet. Appeiere eller apputviklere har derfor fremdeles et stort forbedringspotensial med hensyn til å gjøre informasjon om personvern lettere tilgjengelig fra appen.

¹⁰ <http://www.datatilsynet.no/Teknologi/Apper/app/>

5. Oppsummering – fortsatt for lite informasjon om bruk av personopplysninger

Informasjon om hvordan appene bruker personopplysninger ser ut til å ha blitt bedre de siste årene. Samtidig viser sveipet at det er langt igjen til alle som bruker apper kan forvente å få enkel og god informasjon om personvern når de vurderer å laste ned en app.

Dagens situasjon er preget av et stort sprik i hvor gode aktørene er til å informere. Kun et fåtall av de som lager eller er ansvarlige for apper er flinke til å informere om personvern. Til tross for at mange virksomheter har en personvernerklæring er denne på langt nær god nok.

En viktig grunn er at det er lagt for lite arbeid i å beskrive hvorfor appene trenger de tilgangene til personopplysninger som de ber om, og hvordan disse opplysningene brukes. Resultatet er at brukeren ikke får god nok informasjon til å ta et bevisst valgt om hun eller han ønsker å gi appen tilgang til sine personopplysninger eller ikke.

En annen grunn er at en del aktører bruker en henvisning til en personvernerklæring som en lettvinnt løsning. De viser rett og slett til en erklæring de hadde fra før, men som ikke inneholder noen spesifikk informasjon til brukerne av appen. Disse virksomhetene har med andre ord en infrastruktur på plass for å kunne gi brukerne god informasjon, som de ikke benytter. De går derfor glipp av en god kanal til å gi brukerne nødvendig informasjon, som igjen vil bygge tillit hos brukerne.

Det mest urovekkende funnet i appsveipet handler imidlertid om de tilgangene vi ikke forstår at appen trenger ut fra den funksjonen den har. 31 prosent av appene vi sjekket bad om en eller flere tilganger i denne kategorien. Her var tallet likt i det norske sveipet og de samlede GPEN-tallene. Vi antar at dette problemet i stor grad skyldes at appen ikke forklarer hvorfor den trenger tilgangen vi ikke forstår hvorfor den ber om. Samtidig antar vi at en del av disse tilgangene representerer reelle misforhold mellom hva appen ber om tilgang til og hva

den trenger av informasjon og tilganger for å gi brukeren tjenesten den tilbyr.

Hva skal til for å bedre situasjonen?

Det er et klart forbedringsbehov i appers informasjon om hvordan de behandler personopplysninger. Når vi vet at de fleste brukere har en rekke ulike apper installert på sine mobile enhet, er det lett å trekke konklusjonen at brukerne ikke er i stand til å ha kontroll over hvilken informasjonen som samles inn gjennom appenes tilganger.

I 2013 vedtok verdens personvernmyndigheter en deklarasjon om apper og personvern¹¹. Denne understreker at forståelig og tilgjengelig informasjon til brukerne er sentralt for å oppnå godt personvern i apper. Det er også behov for tiltak som sikrer at apputviklere arbeider etter prinsippene for innebygd personvern. Sist, men ikke minst må også leverandørene av operativsystem, som Google og Apple, både stille krav til apper og legge til rette for god personvernfunksjonalitet.

I den norske konteksten ser vi at de profesjonelle aktørene, det vil si utviklere og virksomheter som bestiller en app, er sentrale. De må sørge for at godt personvern er et av kravene som legges til grunn når apper utvikles. Man bør legge samme profesjonalitet til grunn ved apputvikling som ved annen programvareutvikling. Bevisste leverandører er grunnleggende for å få til dette. Datatilsynet forventer at sentrale bransjeorganisasjoner bidrar til dette, og vi ønsker dialog med sektoren om dette arbeidet. Våren 2014 lanserte vi en veileder for apputviklere¹² som en hjelp til arbeidet med å sørge for godt personvern i apper.

God informasjon om appers tilganger og bruk av disse, vil bidra positivt til publikums kunnskap om personvern og apper generelt. Samtidig vil det sette brukeren i stand til å selv velge hvilke apper de ønsker å dele opplysningene sine med. Om forbrukerne ønsker å verne om egne personopplysninger, oppfordringer vi dem til å styre unna apper som ikke på en god måte forteller hvilke tilganger de trenger og hvorfor.

¹¹ Warsaw declaration on the "appification" of society https://privacyconference2013.org/web/pageFiles/kcfinder/files/AT_T29312.pdf

¹² <https://www.datatilsynet.no/Teknologi/Apper/Mobilt-personvern/>

VEDLEGG 1: Sveipeskjema

Skjemaet er en oversettelse av den engelske versjonen fra koordinator for sveipet. Vi har kun gjort enkelte mindre tilpasninger.

GPEN sveip 2014 – Apper

Navn på sveiper:

APP INFO										
App navn		App selger/utvikler		Plattform (iOS/Android)			Gratis/betal (evt, hvor mye)			
Aldersbegrensning (vurdering)		Kategori		Land (behandlingsansvarlig) (norsk, utenlandsk)						
INFORMASJON FØR NEDLASTING										
Gir beskrivelsen i appbutikken tilgang til en personvernerklæring? (ja/nei)			Hvis ikke pv.erklæring i selve appbeskrivelse:				Beskriver pv.erklæringen <i>appens</i> bruk av pers.opplysninger (ikke bare beh.ansvarligs generelle beh. av pers.opplysn.)? (ja/nei)			
			Finnes det en pv.erkl. på appselgers/beh.ansvarligs nettside? (ja/nei/NA)							
TILGANGER – (j/n/-)			Skriv en strek i gult og grønt felt hvis appen ikke ber om tilgang:							
	Lokasjon	Kontakter	Kalender	Mikrofon	Kamera	Enhetsidentifikator (IMEI, tlfnr, serienr)	Tilgang til andre kontoer	SMS	Tlf logg	Annet (spesifikke)

[illegible]

ETTER INNSTALLERING – (ja/nei)				
Er det en personvernerklæring (el. lenke til) i appen?		Hvis ja, er informasjonen i erklæringen spesifikk for appen?		Er informasjonen om personvern i appen tilpasset smarttelefon-formatet (pop-ups og lignende)?
Har du sett reklame i appen?	Ble du bedt om å logge inn?	Var du nødt til å logge inn?	Hvis du var nødt til å logge inn: Ble du spurt om å lage ny konto, logge inn på eksisterende konto (FB, Google osv), eller gitt begge valg?	
Kommentarer – Positive observasjoner			Bekymringsfulle observasjoner	

* N/A = Appen samler ikke p.opplysninger

0 = Ingen info om personvern, utover tilganger

1 = Personverninfo om tilganger ikke tilfredstillende; sveiperen vet ikke hvordan p.opplysninger blir samlet/brukt/delt.

2 = Personverninfo om tilganger beskriver i noen grad appens innsamling/bruk/deling av p.opplysninger, men sveiperen er fremdeles usikker på noen tilganger.

3 = Personverninfo om tilganger forklarer tydelig hvordan appen samler/bruker/deler p.opplysninger, sveiperen er informert om appens bruk av p.opplysninger.

VEDLEGG 2: Liste over appene i det norske sveipet

APP INFO				
Appnavn	Appselger/-utvikler	iOS (o) /Android(1)	Gratis(o)/ Betal (1)	Utenlandsk (o)/ norsk (1)
1881	Opplysningen 1881	0	0	1
180.no Mobilsøk + Gratis	180 Mobil AS	1	0	1
Bil og henger	Statens egvesen	1	0	1
Båtførerprøve	Cappelen Damm AS	0	0	1
Camera+	tap tap tap LLC	0	1	0
Dagbladet.no	Dagbladet.no	1	0	1
Del regning	Funkbit AS	0	1	1
Dnb	Dnb ASA	0	0	1
Downhill Supreme 2	Art RR SIA	0	1	0
Dropbox	Dropbox, Inc.	0	0	0
Endomonde Sports Tracker	Endomonde.com	1	0	0
Facebook	Facebook Inc.	0	0	0
Farm Heros Saga	King.com	1	0	0
Finn	finn.no	0	0	1
Flightradar24 Pro	Flightradar24 AB	0	1	0
Geocaching	Groungspeak	1	1	0
Geometry Dach	Robert Topala	0	1	0
gmail	Google Inc.	1	0	0
Google Search	Google Inc.	0	0	0
Gule sider Navigasjon	Eniro	1	0	1
H&M	H&M AB	0	0	0
Hjelp 113-GPS	Stiftelsen Norsk Luftambulanse	0	0	1
Hva er fargen?	Gabriel Silvu Stefan	0	0	0
Instagram	Instagram Inc.	0	0	0
iSikte - Norge	AppsFab AS	0	1	1

Kaloriteller	Appsonite AS	0	1	1
Lifesum	Shapeup Club AB	1	0	0
LinkdIn	LinkdIn	1	0	0
Maps	Google Inc.	1	0	0
Matgelde	Tine BA	0	0	1
Matvaretilbud	Butek	0	0	1
Messenger	Facebook Inc.	0	0	0
Min meny	Norgesgruppen Data AS	0	0	1
Min Sky	Telenor Digital	0	0	1
Minecraft Pocket Edition	Mojang	1	1	0
MinFotball	Funn IT	1	0	1
Monument Vally	Ustwo	0	1	0
Narvesen	Apphuset	0	0	1
Netflix	Netflix Inc.	1	0	0
Nordea for Android	Nordea Bank AB	1	0	0
Norsk Mat	Moten Skjelland	0	0	1
Norsk Mat, Matvaretabellen	Morten Skjellart	0	0	1
Norwegian Reiseassistent	Norwegian	0	0	1
Nrk radio	Nrk	0	0	1
Nrk TV	Nrk	0	0	1
NSB	NSB AS	0	0	1
P4 - Lyden av hele Norge	P4 Radio Hele Norge	0	0	1
QuizDan	Ravn Studio AS	0	1	1
Quizkampen	FED Media AB	0	0	0
Runtastic Pro	Runtastic	0	1	0
Ruter Reise	codebox.no	1	0	1
RuterBillett	Ruter AS	1	0	1
Skadehåndboka prøveversjon	Sigve Dhontup Holmen	0	0	1

Skype for iphone	Skype Communication S.à.r.l.	0	0	0
Slutta	Helsenorge.no	1	0	1
Snapchat	Snapchat, Inc.	0	0	0
SpareBank1 Moblibank	SpareBank1	1	0	1
Spotify Music	Spotify Ltd.	0	0	0
Storm	StormGeo	1	0	1
Studentappen	Eivind Moland	0	0	1
Swiftkey Keyboard	Man Hin Tan/ Axotic	0	1	0
Sykt Barn App	Smart Caring	0	1	1
Telefonterror	Hinderberg	0	1	1
Twitter	Twitter Inc.	1	0	0
Ukenummer for alltid	Trond Rossvoll	0	1	1
Ut.no turguide	Nrk	0	0	1
VG	VG Mobil	0	0	1
Viber	Viber Media S.à.r.l.	1	0	0
Wolfram Alpha	Wolfram Alpha, LLC	1	1	0
Wordfeud	Bertheussen IT	1	1	0
You Tube	Google Inc.	1	0	0
Yr	Nrk	0	0	1

VEDLEGG 3: Land og personvernmyndigheter som deltok i GPEN Privacy Sweep 2014

Australia:	Office of the Australian Information Commissioner og Office of the Victorian Privacy Commissioner
Belgia:	Privacy Commission of Belgium
Canada:	The Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner of British Columbia og Office of the Privacy Commissioner of Canada
Kina:	Office of the Privacy Commissioner for Personal Data, Hong Kong SAR og Office for Personal Data Protection, Macao SAR
Colombia:	Superintendence of Industry and Commerce of Colombia
Estland:	Estonian Data Protection Inspectorate
Finland:	Office of the Data Protection Ombudsman
Frankrike:	Commission Nationale de l'Informatique et des Libertés
Tyskland:	Commissioner for Data Protection Baden-Württemberg, Data Protection Supervisory Authority of Bavaria, Berlin Data Protection Commission og Data Protection Commissioner of Hesse
Gibraltar:	Gibraltar Regulatory Authority
Irland:	Office of the Data Protection Commissioner of Ireland
Israel:	The Israeli Law, Information and Technology Authority (ILITA)
Italia:	Italian Data Protection Authority
Mexico:	Federal Institute for Access to Information and Data Protection
New Zealand:	Office of the Privacy Commissioner
Norge	Datatilsynet
Spain:	Spanish Data Protection Authority
Storbritannia:	The Information Commissioner's Office
USA:	Federal Trade Commission



Datatilsynet

Besøksadresse:

Tollbugata 3, 0152 Oslo

Postadresse:

Postboks 8177 Dep., 0034
Oslo

postkasse@datatilsynet.no

Telefon: +47 22 39 69 00

datatilsynet.no

personvernbloggen.no