DATATILSYNET

Justitsministeriet
Slotsholmsgade 10
1216 København K

20. august 2010

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2010-139-0013
2010-131-0033
2010-131-0034
2010-131-0035
2010-131-0036
Sagsbehandler
Vita Hornemann
Direkte 3319 3232

Vedrørende bidrag til besvarelse af spørgsmålet nr. 196 og 197 af 6. juli 2010 fra Udvalget for Videnskab og Teknologi (Alm. del), spørgsmål nr. 1379, 1380, 1381 og 1382 af 29. juli 2010 fra Retsudvalget (Alm. del)

1. I breve af 15. og 30. juli samt 3. august 2010 har Justitsministeriet anmodet Datatilsynet om en udtalelse til brug for besvarelsen af ovennævnte spørgsmål fra Folketingets Udvalg for Videnskab og Teknologi samt Folketingets Retsudvalg.

Spørgsmålene fra Udvalget for Videnskab og Teknologi lyder som følger:

Spørgsmål 196
Finder ministeren, det er uacceptabelt, at Apple registrerer brugere af iPhones GPS-ruter med det formål at sælge dem videre?

Spørgsmål 197
Vil ministeren tage initiativ til at gennemføre de nødvendige ændringer af lovgivningen, så det bliver forbudt for f.eks. Apple at registrere GPS-ruter fra forbrugernes brug af iPhone og at sælge disse oplysninger videre?

Spørgsmålene fra Retsudvalget lyder som følger:

Spørgsmål 1379
Ministeren bedes redegøre for, hvorvidt ministeren vil kræve, at Apple oplyser, hvad de oplysninger, der indsamles via iPhone, anvendes til?

Spørgsmål 1380
Ministeren bedes redegøre for, hvorvidt ministeren ligesom sin tyske kollega vil kræve, at Apple oplyser, hvor længe de oplysninger, der indsamles om brugerne via iPhone, gemmes?

Spørgsmål 1381
Ministeren bedes redegøre for, om Apple og andre tjenesteleverandører er omfattet af dansk lovgivning i forbindelse med logning af lokationsdata hos brugere af bestemte tjenester på eksempelvis iPhone enheder, når disse befinder sig i Danmark?

Spørgsmål 1382
Ved køb af musik og applikationer via Apple kræves accept af Apples nye privacy policy, der tillader Apple at indsamle og gemme lokationsdata. Ministeren bedes redegøre for, hvordan man vil garantere borgerne at kunne bruge deres købte mobile enheder uden at skulle give tilladelse til at blotlægge lokationsdata.

2. I den anledning kan Datatilsynet oplyse følgende:

2.1. Datatilsynet har ikke behandlet spørgsmål vedrørende funktionaliteten i Apples iPhone og har derfor ikke nærmere kendskab hertil.

2.2. Ved opslag på de danskprogede dele af Apples hjemmeside har Datatilsynet fundet Apples "Politik for Behandling af Personlige Oplysninger"[1]. Heri er bl.a. anført:

"Bemærk, at personlige oplysninger om enkeltpersoner med bopæl i et land inden for det europæiske økonomiske samarbejdsområde (EØS) administreres i fællesskab af Apple Sales International i Cork, Irland, og Apple Limited i Uxbrigde, Storbritannien. Personlige oplysninger indsamlet inden for EØS under brug af iTunes administreres af iTunes SARL i Luxembourg."

Tilsvarende oplysninger om dataansvaret gives på telefonsvareren på det danske telefonnummer, der er anført på Apples side med "Betingelser for Apple Store"[2], som tillige henviser til, at kontakt kan ske til en postadresse i Irland.

Umiddelbart ser det således ud til, at dataansvaret for behandlingen af personoplysninger om de danske brugere ligger hos Apple i Irland og Storbritannien.

Når den dataansvarlige findes i et andet EU-land og ikke i Danmark, indebærer persondatalovens regler om geografisk anvendelsesområde, at det er dette lands persondatalovgivning og ikke den danske persondatalov, der finder anvendelse.

3.1. Hvis en virksomhed *er* omfattet af den danske persondatalov, skal virksomhedens behandlinger ske under iagttagelse af bl.a. behandlingsbetingelserne i persondataloven. Disse betingelser svarer i vidt omfang svarer til reglerne i EU's databeskyttelsesdirektiv.

3.2. Kravene til databehandlingen består bl.a. af grundbetingelser, som altid skal være opfyldt. De grundlæggende krav går ud på følgende:

- Når man behandler personoplysninger, skal det ske i overensstemmelse med god databehandlingsskik. Dette indebærer, at den dataansvarlige nøje skal overholde reglerne i loven, såvel i ånd som bogstav, og ikke må forsøge at omgå reglerne.

---

[1] http://www.apple.com/dk/legal/privacy/.

[2] http://storeimages.apple.com/1427/store.apple.com/Catalog/dk/Images/salespolicies_consumer.html

- Når en dataansvarlig samler personoplysninger ind, skal det stå klart, hvilket formål oplysningerne skal bruges til, og formålet skal være sagligt. Det er ikke tilladt at indsamle oplysninger, hvis man ikke aktuelt har noget at bruge dem til, men blot forventer, at der senere viser sig et formål. Om et bestemt formål med en indsamling af personoplysninger er sagligt, afhænger først og fremmest af, om der er tale om løsning af en opgave, som det er naturligt for den pågældende myndighed, virksomhed m.v. at løse. Hvad der er sagligt for den ene myndighed eller virksomhed, vil altså ikke nødvendigvis være sagligt for den anden.

- En senere behandling må ikke være uforenelig med det formål, som oplysningerne oprindeligt blev indsamlet til. Indsamlede oplysninger kan efterfølgende principielt godt anvendes til et andet end det oprindelige formål, blot den senere anvendelse ikke er uforenelig med det formål, som oplysningerne oprindeligt blev indsamlet til. Hvis den senere behandling direkte modarbejder eller skader det oprindelige formål, er det klart, at behandlingen ikke kan finde sted. Herudover må det vurderes konkret, om en senere behandling må anses for så uvedkommende i forhold til det oprindelige formål, at den ikke kan accepteres.

- Indsamlede oplysninger må ikke omfatte mere end nødvendigt, formålet taget i betragtning. Denne regel skal bidrage til at sikre mod en unødvendig ophobning af personoplysninger. Loven bygger altså på det princip, at offentlige myndigheder og private virksomheder m.v. ikke må indsamle og registrere flere oplysninger om den enkelte borger, end hvad der er nødvendigt.

- Den dataansvarlige skal sikre sig, at der ikke behandles urigtige eller vildledende oplysninger. Viser det sig alligevel, at der behandles oplysninger, som er urigtige eller vildledende, skal disse snarest muligt slettes eller rettes. Disse krav skal bidrage til at sikre den bedst mulige datakvalitet.

- Indsamlede oplysninger skal slettes eller anonymiseres, når det ikke længere er nødvendigt for den dataansvarlige at være i besiddelse af oplysningerne i en form, der gør det muligt at identificere den enkelte person. Også denne regel skal sikre mod dataophobning.

3.3. Persondataloven inddeler herudover oplysningerne i tre niveauer eller typer.

Følsomme oplysninger om menneskers rent private forhold. Det drejer sig om oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

Andre typer af oplysninger om rent private forhold anses også for at være følsomme. Det drejer sig om oplysninger om strafbare forhold, væsentlige sociale problemer og lignende følsomme privatlivsoplysninger, f.eks. om interne familieforhold.

De oplysningstyper, der ikke vedrører rent private forhold, kan kaldes almindelige personoplysninger. Almindelige personoplysninger kan f.eks. være identifikationsoplysninger, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke følsomme oplysninger.

3.4. Datatilsynet er bekendt med, at Apple den 12. juli 2010 har svaret på en henvendelse fra to medlemmer af Repræsentanternes Hus i USA. Svaret er tilgængeligt på internettet på denne adresse:
http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf

Ud fra dette må det umiddelbart lægges til grund, at de oplysninger, som Apple behandler, falder i kategorien almindelige personoplysninger.

Behandling af almindelige personoplysninger må efter persondataloven ske, når en af følgende betingelser er opfyldt:

1) Hvis den registrerede har givet sit udtrykkelige samtykke. Kravet om udtrykkelighed betyder, at et stiltiende eller indirekte samtykke ikke er tilstrækkeligt.

2) Hvis behandlingen er nødvendig for at kunne opfylde en aftale, som den registrerede er part i. F.eks. kan det være nødvendigt at registrere og behandle oplysninger, der fremgår af ordrer, fakturaer og lignende i tilknytning til aftaler, hvor den registrerede er aftalepart.

3) Hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige. En retlig forpligtelse kan eksempelvis være en forpligtelse, der er fastsat i en lov eller en bekendtgørelse.

4) Hvis behandlingen er nødvendig for at beskytte den registreredes vitale interesser. F.eks. kan behandling af oplysninger ske, hvis den registrerede som følge af bortrejse eller sygdom ikke er i stand til at give samtykke til behandlingen. Det er en betingelse, at behandlingen vedrører interesser, der er af fundamental betydning for den registrerede.

5) Hvis behandlingen er nødvendig for at kunne udføre en opgave i samfundets interesse. Dermed vil behandling af oplysninger til gavn for en bredere kreds af personer, eksempelvis i statistisk, historisk, informativt eller videnskabeligt øjemed kunne ske.

6) Hvis behandlingen sker som led i myndighedsudøvelse. Det er først og fremmest tilfældet, når offentlige myndigheder træffer afgørelser i forvaltningssager, f.eks. afgørelser om sociale ydelser eller afgørelser om skatteansættelser.

7) Hvis behandlingen er nødvendig for at varetage en berettiget interesse, og denne interesse overstiger hensynet til den registreredes interesser. Den dataansvarlige skal, før vedkommende behandler data, vurdere, hvorvidt hensynet til de interesser, der ønskes forfulgt med behandlingen, overstiger den registreredes interesser. Denne vurdering afhænger af mange forskellige forhold, bl.a. formålet med behandlingen. F.eks. er det tilladt at føre sædvanlige personaleregistre og registre over en virksomheds kunder og leverandører.

4. Datatilsynet fører tilsyn med enhver behandling, der omfattes af persondataloven, bortset fra behandlinger, der foretages for domstolene.

I forbindelse hermed påser Datatilsynet af egen drift eller efter klage fra en registreret, at en behandling finder sted i overensstemmelse med lovgivningen og de bestemmelser, der er udstedt i medfør af loven.

Som led i denne tilsynsvirksomhed kan Datatilsynet tage sager op af egen drift, hvis tilsynet finder grundlag herfor.

Ud fra de oplysninger, som Apple har givet i det omtalte svar af 12. juli 2010 til medlemmer af Repræsentanternes Hus, finder Datatilsynet ikke umiddelbart grundlag for at indlede en nærmere undersøgelse i sagen.

Datatilsynet lægger i denne forbindelse særligt vægt på følgende:

- Der er ifølge det oplyste mulighed for at slå alle lokationsbaserede tjenester fra med en enkelt indtastning.
- Apple anmoder ifølge det oplyste om udtrykkeligt samtykke fra brugeren, når en applikation eller webside anmoder om lokationsbaseret information første gang. Når en applikation eller webside anmoder om informationer, viser der sig en dialogboks med indholdet: "[Application/Website] would like to use your current location." Brugeren spørges: "Don't Allow" eller "OK". Hvis brugeren klikker på "Don't allow" vil ingen lokationsbaseret information ifølge det oplyste blive indsamlet eller transmitteret.
- Apples persondatapolitik, som er opdateret 21. juni 2010, beskriver behandling af personoplysninger i forbindelse med lokationsbaserede tjenester. Politikken er tilgængelig på dansk[3], og der er link til dokumentet på Apples dansksprogede sider.

Datatilsynet henviser i øvrigt til Apples brev af 12. juli 2010 for nærmere detaljer om databehandlingen.

Datatilsynet vil følge udviklingen og holde sig orienteret om eventuelle spørgsmål vedrørende behandlingen af lokationsdata, som behandles af datatilsynene i andre EU-lande.

---

[3] http://www.apple.com/dk/legal/privacy/

5. Datatilsynet har ikke grundlag for at vurdere, om de omtalte køb af musik og andre applikationer via Apple rejser spørgsmål i forhold til forbrugerlovgivningen, herunder reglerne på markedsføringsområdet.

Med venlig hilsen

Janni Christoffersen
Direktør

Politik for Behandling af Personlige Oplysninger

Det er vigtigt for Apple at beskytte din identitet. Derfor har vi udarbejdet en Politik for Behandling af Personlige Oplysninger, der indeholder retningslinjer for, hvordan vi indsamler, bruger, udleverer, overfører og gemmer dine oplysninger. Vi beder dig om at bruge et øjeblik til at sætte dig ind i vores praksis for behandling af personlige oplysninger og lade os vide, hvis du har nogen spørgsmål.

TRUSTe
ANERKENDT PRIVATLIV

Apple, Inc. er blevet tildelt TRUSTe's "Privacy Seal", hvilket viser, at denne Politik for Behandling af Personlige Oplysninger og vores praksis er blevet gennemgået af TRUSTe for at sikre, at kravene til TRUSTe's program er opfyldt, herunder vedrørende gennemsigtighed, ansvarlighed og valg ved indsamling og brug af dine personlige oplysninger. TRUSTe-programmet dækker ikke information, som eventuelt indsamles igennem software, der kan downloades. Hvis du har spørgsmål til eller vil klage over vores Politik for Behandling af Personlige Oplysninger eller vores praksis, bedes du kontakte os via privacy@apple.com. Hvis du ikke er tilfreds med vores svar, kan du kontakte TRUSTe her .

Indsamling og brug af personlige oplysninger

Personlige oplysninger er data, som kan bruges til entydigt at identificere eller kontakte en bestemt person.

Du kan blive bedt om at afgive dine personlige oplysninger på ethvert tidspunkt, når du er i kontakt med Apple eller et Apple-associeret selskab. Apple og Apples associerede selskaber kan udveksle disse personlige oplysninger med hinanden og bruge dem i overensstemmelse med denne Politik for Behandling af Personlige Oplysninger. De kan også kombinere dem med andre oplysninger for at udbyde og forbedre vores produkter, tjenester, indhold og annoncering.

Her er nogle eksempler på, hvilken type personlige oplysninger Apple kan indsamle, og hvordan vi kan bruge dem.

Personlige oplysninger, vi indhenter

- Når du opretter en Apple ID, registrerer dine produkter, ansøger om kredit, køber et produkt, downloader en softwareopdatering, registrerer dig i en klasse i en Apple Retail Store eller deltager i en onlineundersøgelse, kan vi indsamle forskellige oplysninger, herunder dit navn, postadresse, telefonnummer, e-mailadresse og kreditkortoplysninger, samt hvordan du ønsker at blive kontaktet.
- Når du deler dit indhold med familie og venner ved brug af et Apple-produkt, sender gavecertifikater og produkter eller inviterer andre til at tilslutte sig på Apples fora, kan Apple indsamle de oplysninger, du giver om disse personer, såsom navn, postadresse, e-mailadresse og telefonnummer.
- I USA kan vi bede dig om dit Social Security number (SSN), men kun under begrænsede omstændigheder, som fx når du opretter en trådløs konto, aktiverer din iPhone eller med henblik på, om der kan bevilges længere kredittid.

Hvordan vi bruger dine personlige oplysninger

- De personlige oplysninger, vi indsamler, gør det muligt for os at holde dig orienteret om Apples seneste produkter, softwareopdateringer og kommende begivenheder. De hjælper os også til at forbedre vores tjenester, indhold og annoncering. Hvis du ikke ønsker at være på vores mailingliste, kan du til enhver tid framelde dig ved at opdatere dine indstillinger.
- Dine personlige oplysninger hjælper os også til at udvikle, levere og forbedre vores produkter, tjenester, indhold og annoncering.
- Undertiden kan vi bruge dine personlige oplysninger til at sende dig vigtige beskeder om køb eller ændringer af vores vilkår, betingelser og politikker. Da disse oplysninger er vigtige for dit forhold til Apple, kan du ikke fravælge at modtage disse meddelelser.
- Vi kan også bruge de personlige oplysninger til interne formål, såsom revidering, analyser og forskning, så vi kan forbedre Apples produkter, tjenester og kundekommunikation.
- Hvis du deltager i et lotteri, en konkurrence eller lignende promotion, kan vi bruge de oplysninger, du giver, til at administrere sådanne programmer.

Indsamling og brug af ikke-personlige oplysninger

Vi kan også indsamle ikke-personlige oplysninger, dvs. data i en form, som ikke kan sættes i direkte forbindelse med specifikke personer. Vi kan indsamle, bruge, overføre og udlevere ikke-personlige oplysninger til ethvert formål. Her er nogle eksempler på, hvilken type ikke-personlige oplysninger Apple kan indsamle, og hvordan vi kan bruge dem:

- Vi kan indsamle oplysninger om stilling, sprog, postnummer, områdenummer, enhedens unikke identifikationsnummer, hvor og i hvilken tidszone Apple-produktet bruges, så vi bedre kan forstå brugeradfærden og forbedre vores produkter, tjenester og annoncering.
- Vi kan også indsamle oplysninger om kundernes aktiviteter på vores websted, på tjenesterne MobileMe og iTunes Store og fra vores andre produkter og tjenester. Disse oplysninger sammenføres og hjælper os til at give en mere nyttig information til vores kunder og til at forstå, hvilke områder af vores websted, produkter og tjenester, der er mest populære. Sammenførte data betragtes som ikke-personlige oplysninger med henblik på denne Politik for Behandling af Personlige Oplysninger.

Hvis vi kombinerer ikke-personlige oplysninger med personlige oplysninger, vil de kombinerede oplysninger blive behandlet som personlige oplysninger, så længe de forbliver kombinerede.

Cookies og andre teknologier

Apples websted, onlinetjenester, interaktive applikationer, e-mailbeskeder og annoncering kan anvende "cookies" og andre teknologier såsom pixel tags og web beacons. Disse teknologier hjælper os til bedre at forstå brugeradfærden og fortæller os, hvilke områder af vores websted, der er mest populære, ligesom de gør det lettere at måle effektiviteten af annoncer og web-søgninger. Vi behandler oplysninger indhentet via cookies og andre teknologier som ikke-personlige oplysninger. I det omfang IP-adresser og lignende identifikation betragtes som personlige oplysninger ifølge lokal lovgivning, vil vi dog også behandle denne identifikation som personlige oplysninger. I det omfang ikke-personlige oplysninger kombineres med personlige oplysninger, vil vi på lignende måde behandle de kombinerede oplysninger som personlige oplysninger med henblik på denne Politik for Behandling af Personlige Oplysninger.

Apple og Apples partnere bruger cookies og andre teknologier i mobile annonceringstjenester til at kontrollere, hvor mange gange du ser en given ad, levere ads, som har relation til dine interesser, og måle

effektiviteten af ad-kampagner. Hvis du ikke ønsker at modtage ads med dette relevansniveau på din mobile enhed, kan du framelde dig ved at gå ind på følgende link på din enhed. http://oo.apple.com. Hvis du fravælger, vil du fortsat modtage samme antal mobile ads, men de kan være mindre relevante, fordi de ikke vil være baseret på dine interesser. Du kan stadig se ads, der relaterer sig til indholdet på et websted eller i en applikation, eller som er baseret på andre ikke-personlige oplysninger. Dette fravalg gælder kun for Apples annonceringstjenester og har ingen indflydelse på interessebaseret annoncering fra andre annonceringsnetværk.

Apple og vores partnere bruger også cookies og andre teknologier til at huske personlige oplysninger, når du bruger vores websted, onlinetjenester og applikationer. Vores mål er i disse tilfælde at gøre din oplevelse med Apple mere målrettet og personlig. Hvis vi fx kender dit fornavn, kan vi byde dig velkommen, næste gang du besøger Apple Online Store. Oplysninger om dit land og sprog – og din skole, hvis du er underviser – hjælper os til at give dig en mere målrettet indkøbstur på nettet. Hvis vi ved, at nogen, der bruger din computer eller enhed, har købt et bestemt produkt eller brugt en særlig tjeneste, hjælper det os til at gøre vores annoncering og e-mailkommunikation mere relevant for dine interesser. Og dine kontaktoplysninger, produkternes serienummer og oplysning om din computer eller enhed hjælper os til at registrere dine produkter, tilpasse dit operativsystem, opsætte din MobileMe-tjeneste og yde dig en bedre kundeservice.

Hvis du ønsker at slå cookies fra, og du bruger Safari web browser, skal du gå til Safari foretrukne indstillinger og derefter til sikkerhedsfeltet for at slå cookies fra. På din mobile Apple-enhed skal du gå til Indstillinger, derefter til Safari og herefter til Cookies-sektionen. For andre browsere, kontroller hos din udbyder, hvordan du slår cookies fra. Bemærk, at visse funktioner på Apples websted ikke vil være tilgængelige, når cookies er slået fra.

Som det er tilfældet for de fleste websteder, indsamler vi visse oplysninger automatisk og opbevarer dem i logarkiver. Disse oplysninger inkluderer IP-adresser, browsertype og sprog, Internetudbyder (ISP), henvisnings- og udgangssider, operativsystem, dato-/tidsstempel og navigationsdata.

Vi bruger disse oplysninger til at forstå og analysere tendenser, administrere webstedet, få viden om brugeradfærden på webstedet og til at indsamle demografiske oplysninger om vores brugere som helhed. Apple kan bruge disse oplysninger i vores markedsførings- og annonceringstjenester.

I nogle af vores henvendelser via e-mail bruger vi den såkaldte "click-through URL" der er linket til indholdet på Apple-webstedet. Når kunderne klikker på en af disse URL-adresser, passerer de gennem en separat webserver, før de kommer ind på den relevante side på vores websted. Vi sporer disse click-through data for at finde ud af, hvilke emner, der interesser dig, og til at måle om vores kundekommunikation er logisk og brugervenlig. Hvis du ikke vil have dine bevægelser registreret på denne måde, skal du blot undlade at klikke på henvisninger til tekst eller grafik i e-mailbeskeden.

Pixel tags giver os mulighed for at sende e-mailbeskeder i et format, som kunderne kan læse, og de fortæller os, om beskederne er blevet åbnet. Vi kan bruge disse oplysninger til at sende færre eller slet ingen beskeder til en kunde.

Udlevering til tredjeparter

I visse situationer kan Apple stille visse personlige oplysninger til rådighed for strategiske partnere, der samarbejder med Apple om at udbyde produkter og tjenester, eller som hjælper Apple med at markedsføre sig over for kunderne. Når du køber og aktiverer din iPhone, giver du fx Apple og operatøren lov til at udveksle de oplysninger, du opgiver under aktiveringsprocessen, med henblik på at levere tjenesten. Hvis du bliver godkendt, vil din konto være underlagt Apples og operatørens respektive politik for behandling af personlige oplysninger. Apple vil kun dele dine personlige oplysninger for at udbyde og forbedre vores produkter, tjenester og annoncering, og de vil ikke blive delt med tredjeparter til deres markedsføringsformål.

Tjenesteudbydere
Apple deler personlige oplysninger med firmaer, som udbyder tjenester, såsom behandling af oplysninger, forlængelse af kredittider, ekspedition af ordrer fra kunder, levering af produkter til dig, behandling og forbedring af kundedata, ydelse af kundeservice, vurdering af din interesse i vores produkter og tjenester samt gennemførelse af kunde- og tilfredshedsundersøgelser. Disse firmaer er forpligtet til at beskytte dine oplysninger og kan lokaliseres overalt, hvor Apple opererer.

Andre
Apple kan i visse tilfælde være pålagt at udlevere dine personlige oplysninger i kraft af lovgivningen eller af en retskendelse og/eller et påbud fra offentlige eller statslige myndigheder i eller uden for dit bopælsland. Vi kan også udlevere oplysninger om dig, hvis vi vurderer, at det er nødvendigt af hensyn til den nationale sikkerhed, overholdelse af loven eller af andre hensyn til den offentlige interesse.

Vi kan også udlevere oplysninger om dig, hvis vi vurderer, at udlevering er begrundet og nødvendig for at håndhæve vores vilkår og betingelser eller beskytte vores virksomhed eller brugere. I tilfælde af reorganisering, fusion eller salg kan vi overføre enhver og alle personlige oplysninger, som vi indsamler, til den pågældende tredjepart.

Beskyttelse af personlige oplysninger

Apple træffer de fornødne administrative, tekniske og fysiske sikkerhedsforanstaltninger for at beskytte dine personlige oplysninger mod tab, tyveri og misbrug samt uautoriseret adgang, udlevering, ændring og destruktion.

Apples onlinetjenester såsom Apple Online Store og iTunes Store benytter SSL-kryptering (Secure Sockets Layer) på alle websteder, hvor der indsamles personlige oplysninger. Hvis du vil købe et produkt fra disse tjenester, skal du bruge en browser, som understøtter SSL, fx Safari, Firefox eller Internet Explorer. Derved beskyttes dine fortrolige personlige oplysninger, når de sendes via Internet.

Når du bruger visse af Apples produkter, tjenester eller applikationer eller indsender indlæg til et Apple-forum, benytter et chatroom eller sociale netværkstjenester, vil de personlige oplysninger, du deler, være synlige for andre brugere, som kan læse, indsamle og bruge dem. Du er ansvarlig for de personlige oplysninger, du vælger at sende i disse tilfælde. Hvis du fx angiver dit navn og din e-mailadresse, når du sender indlæg til et forum, vil disse oplysninger være offentlige. Vær derfor forsigtig, når du bruger disse funktioner.

Dine personlige oplysningers integritet og opbevaring

Apple gør det let for dig at holde dine personlige oplysninger korrekte, fuldstændige og ajourførte. Vi vil opbevare dine personlige oplysninger i den periode, der er nødvendig for at opfylde de formål, der er anført i denne Politik for Behandling af Personlige Oplysninger, medmindre en længere periode kræves eller er tilladt ifølge loven.

Adgang til personlige oplysninger

Du kan hjælpe os med at sikre, at dine kontaktoplysninger og indstillinger er korrekte, fuldstændige og ajourførte ved at logge ind på din konto på www.apple.com/contact/myinfo. Hvad angår andre personlige oplysninger, bestræber vi os i god tro på at give dig adgang til, at du kan anmode om, at vi korrigerer data, som er ukorrekte, eller sletter data, hvis Apple ikke er nødsaget til at opbevare dem ifølge loven eller af lovlige forretningsformål. Vi kan afvise at behandle anmodninger, som fremsættes et urimeligt antal gange, kræver uforholdsmæssige tekniske tiltag, bringer andres privatliv i fare, er ekstremt vanskeligt gennemførlige, eller til hvilke der i øvrigt ikke kræves adgang ifølge den lokale lovgivning. Anmodninger om adgang, korrektion eller sletning kan rettes til den regionale Privacy email addresse.

Børn

Vi indsamler ikke bevidst personlige oplysninger fra børn under 13 år. Hvis vi får kendskab til, at vi har indsamlet personlige oplysninger om et barn under 13 år, vil vi tage skridt til at slette disse oplysninger så hurtigt som muligt.

Lokationsbaserede tjenester

For at kunne yde lokationsbaserede tjenester på Apple-produkter, kan Apple og vores partnere og licenshavere indsamle, bruge og dele præcise lokationsdata, herunder real-time geografisk lokation for din Apple-computer eller -enhed. Disse lokationsdata indsamles anonymt i en form, som ikke identificerer dig personligt, og bruges af Apple og vores partnere og licenshavere til at udbyde og forbedre lokationsbaserede produkter og tjenester. For eksempel kan vi dele geografisk lokation med applikationsudbydere, når du tilvælger deres lokationstjenester.

Til visse lokationsbaserede tjenester, der tilbydes af Apple, såsom MobileMe, "Find My iPhone", er dine personlige oplysninger nødvendige for at faciliteterne kan fungere.

Tredjeparters websteder og tjenester

Apples websteder, produkter, applikationer og tjenester kan indeholde links til tredjeparters websteder, produkter og tjenester. Vores produkter og tjenester kan også anvende eller tilbyde produkter eller tjenester fra tredjeparter - fx tredjeparters iPhone applikationer. Oplysninger, der indsamles af tredjeparter, som kan indeholde oplysninger fx om lokationsdata eller kontaktoplysninger, reguleres af deres praksis for behandling af personlige oplysninger. Vi opfordrer dig til at sætte dig ind i disse tredjeparters praksis for behandling af personlige oplysninger.

Internationale brugere

De oplysninger, du giver, kan blive overført eller tilgået af enheder i hele verden, som beskrevet i denne Politik for Behandling af Personlige Oplysninger. Apple opfylder kravene i "safe harbor" programmet, der er udarbejdet af Handelsministeriet i USA, med hensyn til indsamling, brug og opbevaring af personlige oplysninger indsamlet af organisationer i EU og Schweiz. Læs mere om USA's Handelsministeriums program Safe Harbor.

Bemærk, at personlige oplysninger om enkeltpersoner med bopæl i et land inden for det europæiske økonomiske samarbejdsområde (EØS) administreres i fællesskab af Apple Sales International i Cork, Irland, og Apple Limited i Uxbrigde, Storbritannien. Personlige oplysninger indsamlet inden for EØS under brug af iTunes administreres af iTunes SARL i Luxembourg.

Vores interne regler om beskyttelse af dine personlige oplysninger

For at sikre at personlige oplysninger forbliver fortrolige, udleveres vores retningslinjer om beskyttelse af personlige oplysninger og sikkerhed til Apples medarbejdere, og vi håndhæver på det strengeste vores forholdsregler om beskyttelse af personlige oplysninger inden for firmaet.

Spørgsmål om beskyttelse af personlige oplysninger

Hvis du har spørgsmål eller er bekymret over Apples Politik om Beskyttelse af Personlige Oplysninger og behandling af data, kan du skrive til din lokale Apple Data Controller på den e-mailadresse, der gælder for dit land (se listen nedenfor).

Land eller område	**Kontaktoplysninger**
USA	privacy@apple.com
Canada	privacy-ca@apple.com
Latinamerika	privacy-la@apple.com

Europa	privacyeurope@apple.com
Japan	privacy-japan@apple.com
Australien	privacy@apple.com.au
Asien/Stillehavsområdet	privacy@asia.apple.com

Apple kan opdatere sin Politik om Beskyttelse af Personlige Oplysninger løbende. Når der sker væsentlige ændringer i politikken, vil det blive offentliggjort på vores websted sammen med den opdaterede Politik om Beskyttelse af Personlige Oplysninger..

Apple Inc., 1 Infinite Loop, Cupertino, California, USA 95014

Senest opdateret: 21. juni 2010

July 12, 2010

VIA HAND DELIVERY

The Honorable Edward J. Markey
The Honorable Joe Barton
United States House of Representatives
Washington, DC 20515

Re: ***Apple Inc.'s Response to Request for Information Regarding Its Privacy Policy and Location-Based Services***

Dear Representatives Markey and Barton:

I write in response to your June 24, 2010 letter to Steve Jobs requesting information and documents about Apple's privacy policy and location-based services. I appreciate the opportunity to provide additional information about these matters, and I welcome further discussions with you.

To provide context to our responses to the questions presented in your letter, I first would like to provide some background information about Apple's privacy policy, location-based services, the iAd network, and the App Store.

I. APPLE'S PRIVACY POLICY

A. Overview

Apple is strongly committed to protecting the privacy of its customers. Apple has a single Customer Privacy Policy (the "Policy") that applies across all Apple businesses and products, including the iTunes Store and App Store.[1] The Policy, written in easy-to-read language, details what information Apple collects and how Apple and its partners and licensees may use the information. The Policy is available from a link on every page of Apple's website.[2]

As noted in your letter, the Policy was updated on June 21, 2010, to add, among other changes discussed below, the following provision regarding location-based information:

---

[1] As used in the policy and in this letter, "Apple," refers to Apple Inc. and affiliated companies.
[2] The links take customers to http://www.apple.com/legal/privacy, which may also be accessed by customers directly.

> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.
>
> Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.

This provision incorporated similar language regarding location-based information that appears in Apple End User Software License Agreements ("SLAs") for products that provide location-based services. For example, the current iPhone 3GS SLA, last updated in May 2009, states:

> Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data collected by Apple is collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide location-based products and services. **By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data to provide such products and services.** You may withdraw this consent at any time by not using the location-based features or by turning off the Location Services setting on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party applications or services on the iPhone that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services.

(Emphasis in original.) Similar provisions regarding location-based information appear in the iPhone 4, iPad, iPod Touch, Mac OS X, and Safari 5 SLAs.

The Policy identifies dedicated email addresses for privacy-related inquiries and comments. Apple monitors these email addresses and responds to appropriate inquiries in a

timely manner. Customers may also address privacy concerns to TRUSTe, Apple's third-party privacy monitor. A link to TRUSTe is displayed within the Policy.

B. June 2010 Policy Update

In the past three years, Apple revised its Policy three times: June 29, 2007, early February 2008, and June 21, 2010.

The June 29, 2007 update advised customers about the necessary exchange of information between Apple and the relevant cellular carrier when an iPhone is activated. Apple also added a provision stating that it does "not knowingly collect personal information from children." The provision explained that if such information was collected inadvertently, Apple would attempt to delete it "as soon as possible."

The February 2008 Policy update revised language regarding Apple's use of "pixel tags." Pixel tags are tiny graphic images used to determine what parts of Apple's website customers visited or to measure the effectiveness of searches performed on Apple's website. The revised language stated that: "[Apple] may use this information to reduce or eliminate messages sent to a customer."

On June 21, 2010, Apple updated the Policy to incorporate the language regarding location-based services from Apple SLAs, as discussed above. Apple also added provisions regarding new Apple services, such as Apple's MobileMe "Find My iPhone" feature and the iAd network. Apple made the following, additional material changes to the Policy:

- Revised provisions regarding (i) what information Apple collects from customers and how Apple and its partners and licensees may use the information, (ii) the use of "Cookies and Other Technologies," (iii) the safeguards in place to prevent the collection of personal information from children, and (iv) the collection and use of information from international customers; and

- Added provisions (i) advising customers to review the privacy practices of third-party application providers and (ii) cautioning customers about posting personal information on an Apple forum, chat room, or social networking service.

As noted above, customers may access the updated Policy from every page on Apple's website. The updated Policy also was placed where Apple believed the largest number of customers would see it: the iTunes Store. Following the update, every customer logging onto the iTunes Store is prompted to review the iTunes Store Terms and Conditions. For customers with existing iTunes accounts, the webpage states:

> iTunes Store Terms and Conditions have changed. Apple's Privacy Policy
>
> The changes we have made to the terms and conditions include the following:

• Apple's Privacy Policy has changed in material ways. Please visit www.apple.com/legal/privacy or view below.

Customers are asked to click an unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not agree to the Terms and Conditions and the Policy will not be able to use the iTunes Store (*e.g.*, will not be able to make purchases on the iTunes Store or the App Store), but they may continue to use iTunes software.

Customers attempting to open a new iTunes account are directed to a webpage titled: "iTunes Store Terms & Conditions and Apple's Privacy Policy." They are asked to click the same unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not accept the Terms and Conditions and the Policy will not be able to open an iTunes account but may still activate and use their devices.

II. LOCATION-BASED SERVICES

A. Overview

In response to increasing customer demand, Apple began to provide location-based services in January 2008. These services enable applications that allow customers to perform a wide variety of useful tasks such as getting directions to a particular address from their current location, locating their friends or letting their friends know where they are, or identifying nearby restaurants or stores.

Apple offers location-based services on the iPhone 3G, iPhone 3GS, iPhone 4, iPad Wi-Fi + 3G, and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, iPod touch, Mac computers running Snow Leopard,[3] and Windows or Mac computers running Safari 5.[4]

Although Apple's customers value these services and may use them on a daily basis, Apple recognizes that some customers may not be interested in such services at all times. As discussed below, Apple provides its customers with tools to control if and when location-based information is collected from them.

B. Privacy Features

Apple has always provided its customers with the ability to control the location-based service capabilities of their devices. In fact, Apple now provides customers even greater control

---

[3] All of Apple's Mac computers, *e.g.*, MacBook, MacBook Pro, MacBook Air, iMac, Mac mini, and Mac Pro, run on its proprietary Mac OS operating system. Apple released the current version, Mac OS X version 10.6, known as "Snow Leopard," on August 28, 2009.

[4] Safari is Apple's proprietary Internet browser. Apple released the current version of Safari version 5, on June 7, 2010.

over such capabilities for devices running the current version of Apple's mobile operating system—iOS 4.[5]

First, customers have always had the ability to turn "Off" all location-based service capabilities with a single "On/Off" toggle switch. For mobile devices, the toggle switch is in the "General" menu under "Settings." For Mac computers running Snow Leopard, the toggle switch is in the "Security" menu under "System Preferences." And for Safari 5, the toggle switch is in the "Security" menu in Safari "Preferences." If customers toggle the switch to "Off," they may not use location-based services, and no location-based information will be collected.

Second, Apple has always required express customer consent when any application or website requests location-based information for the first time. When an application or website requests the information, a dialogue box appears stating: "[Application/Website] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," no location-based information will be collected or transmitted. This dialogue box is mandatory—neither Apple nor third-parties are permitted to override the notification.

Third, iOS 4 permits customers to identify individual applications that may not access location-based information, even though the global location-based service capabilities setting may be toggled to "On." The "General" menu under "Settings" provides an "On/Off" toggle switch for each application. When the switch for a particular application is toggled to "Off," no location-based information will be collected or transmitted for that application. And even if the switch for an application is toggled to "On," the "Don't Allow/OK" dialogue box will request confirmation from the customer the first time that application requests location-based information. Customers can change their individual application settings at any time.

Finally, an arrow icon ( ) alerts iOS 4 users that an application is using or has recently used location-based information. This icon will appear real-time for currently running applications and next to the "On/Off" toggle switch for any application that has used location-based information in the past twenty-four hours.

C. Location-Based Information

To provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. For devices running the iPhone OS versions 1.1.3 to 3.1, Apple relied on (and still relies on) databases maintained by Google and Skyhook Wireless ("Skyhook") to provide location-based services. Beginning with the iPhone OS version 3.2 released in April 2010, Apple relies on its own databases to provide location-

[5] All of Apple's mobile devices run on its proprietary mobile operating system. Apple released the current version, iOS 4, on June 21, 2010. Currently, iOS 4 may be run on the iPhone 3G, iPhone 3GS, iPhone 4, and iPod touch. The iPad Wi-Fi + 3G, iPad Wi-Fi, and older models of the iPhone run on prior versions of Apple's mobile operating system, referred to as iPhone OS. Apple has released iPhone OS versions 1.0 through 3.2.

based services and for diagnostic purposes. These databases must be updated continuously to account for, among other things, the ever-changing physical landscape, more innovative uses of mobile technology, and the increasing number of Apple's customers. Apple always has taken great care to protect the privacy of its customers.

1. Cell Tower and Wi-Fi Information

a. Collections and Transmissions from Apple Mobile Devices

To provide location-based services, Apple must be able to determine quickly and precisely where a device is located. To do this, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points. The information is stored in a database accessible only by Apple and does not reveal personal information about any customer.

Information about nearby cell towers and Wi-Fi access points is collected and sent to Apple with the GPS coordinates of the device, if available: (1) when a customer requests current location information and (2) automatically, in some cases, to update and maintain databases with known location information. In both cases, the device collects the following anonymous information:

- Cell Tower Information: Apple collects information about nearby cell towers, such as the location of the tower(s), Cell IDs, and data about the strength of the signal transmitted from the towers. A Cell ID refers to the unique number assigned by a cellular provider to a cell, a defined geographic area covered by a cell tower in a mobile network. Cell IDs do not provide any personal information about mobile phone users located in the cell. Location, Cell ID, and signal strength information is available to anyone with certain commercially available software.

- Wi-Fi Access Point Information: Apple collects information about nearby Wi-Fi access points, such as the location of the access point(s), Media Access Control (MAC) addresses, and data about the strength and speed of the signal transmitted by the access point(s). A MAC address (a term that does not refer to Apple products) is a unique number assigned by a manufacturer to a network adapter or network interface card ("NIC"). The address provides the means by which a computer or mobile device is able to connect to the Internet. MAC addresses do not provide any personal information about the owner of the network adapter or NIC. Anyone with a wireless network adapter or NIC can identify the MAC address of a Wi-Fi access point. Apple does not collect the user-assigned name of the Wi-Fi access point (known as the "SSID," or service set identifier) or data being transmitted over the Wi-Fi network (known as "payload data").

First, when a customer requests current location information, the device encrypts and transmits Cell Tower and Wi-Fi Access Point Information and the device's GPS coordinates (if available) over a secure Wi-Fi Internet connection to Apple.[6] For requests transmitted from devices running the iPhone OS version 3.2 or iOS 4, Apple will retrieve known locations for nearby cell towers and Wi-Fi access points from its proprietary database and transmit the information back to the device. For requests transmitted from devices running prior versions of the iPhone OS, Apple transmits—anonymously—the Cell Tower Information to Google[7] and Wi-Fi Access Point Information to Skyhook. These providers return to Apple known locations of nearby cell towers and Wi-Fi access points, which Apple transmits back to the device. The device uses the information, along with GPS coordinates (if available), to determine its actual location. Information about the device's actual location is not transmitted to Apple, Skyhook, or Google. Nor is it transmitted to any third-party application provider, unless the customer expressly consents.

Second, to help Apple update and maintain its database with known location information, Apple may also collect and transmit Cell Tower and Wi-Fi Access Point Information automatically. With one exception,[8] Apple automatically collects this information only (1) if the device's location-based service capabilities are toggled to "On" and (2) the customer uses an application requiring location-based information. If both conditions are met, the device intermittently and anonymously collects Cell Tower and Wi-Fi Access Point Information from the cell towers and Wi-Fi access points that it can "see," along with the device's GPS coordinates, if available. This information is batched and then encrypted and transmitted to Apple over a Wi-Fi Internet connection every twelve hours (or later if the device does not have Wi-Fi Internet access at that time).

b. Collections and Transmissions from Computers Running Snow Leopard and/or Safari 5

Apple collects Wi-Fi Access Point Information when a Mac computer running Snow Leopard makes a location-based request—for example, if a customer asks for the current time

---

[6] Requests sent from devices running older versions of the iPhone OS also include a random identification number that is generated by the device every ninety days. This number cannot be used to identify any particular user or device.

[7] For GPS-enabled devices running prior versions of the iPhone OS, Apple also sends the device's GPS coordinates, if available, anonymously to Google so that Google can update its database of known locations.

[8] For GPS-enabled devices with location-based service capabilities toggled to "On," Apple automatically collects Wi-Fi Access Point Information and GPS coordinates when a device is searching for a cellular network, such as when the device is first turned on or trying to re-establish a dropped connection. The device searches for nearby Wi-Fi access points for approximately thirty seconds. The device collects anonymous Wi-Fi Access Point Information for those that it can "see." This information and the GPS coordinates are stored (or "batched") on the device and added to the information sent to Apple. None of the information transmitted to Apple is associated with a particular user or device.

zone to be set automatically. The information is collected anonymously and is stored in a database accessible only by Apple. Snow Leopard users can prevent the collection of this information by toggling the "Location Services" setting to "Off" in the "Security" menu under "System Preferences."

Apple also provides location-based services in Safari 5. When a customer is using Safari 5 and runs an Internet application that requests location-based information (*e.g.*, Google Maps), a dialog box will appears stating: "[Website name] would like to use your computer location." If the customer selects "Don't Allow," no location-based information is transmitted by the computer. If the customer selects "OK," Wi-Fi Access Point Information is transmitted to Apple with the request, so that Apple can return information about the computer's location. Apple does not store any Wi-Fi Access Point Information sent with requests from Safari 5.

2. Diagnostic Information

To evaluate and improve the performance of its mobile hardware and operating system, Apple collects diagnostic information from randomly-selected iPhones and analyzes the collected information. For example, when an iPhone customer makes a call, Apple may determine the device's approximate location at the beginning and end of the call to analyze whether a problem like dropped calls is occurring on the same device repeatedly or by multiple devices in the same area. Apple determines the approximate location by collecting information about nearby cell towers and Wi-Fi access points and comparing that with known cell tower and Wi-Fi access point locations in Apple's database. Apple may also collect signal strength information to identify locations with reception issues.

Before any diagnostic information is collected, the customer must provide express consent to Apple. If the customer consents, the information is sent to Apple over a secure connection. The information is sent anonymously and cannot be associated with a particular user or device. The diagnostic information is stored in a database accessible only by Apple. If the customer does not consent, Apple will not collect any diagnostic information.

3. GPS Information

The iPhone 3G, iPhone 3GS, iPhone 4, and iPad Wi-Fi + 3G are equipped with GPS chips. A GPS chip attempts to determine a device's location by analyzing how long it takes for satellite signals to reach the device. Through this analysis, the GPS chip can identify the device's latitude/longitude coordinates, altitude, speed and direction of travel, and the current date and time where the device is located ("GPS Information").

Apple collects GPS Information from mobile devices running the iPhone OS 3.2 or iOS 4. GPS Information may be used, for example, to analyze traffic patterns and density in various areas. With one exception,[9] Apple collects GPS Information only if (1) the location-based

[9] GPS Information is also collected during the short period of time (approximately thirty seconds) when a GPS-enabled device with location-based service capabilities toggled to "On" is

service capabilities of the device are toggled to "On" and (2) the customer uses an application requiring GPS capabilities. The collected GPS Information is batched on the device, encrypted, and transmitted to Apple over a secure Wi-Fi Internet connection (if available) every twelve hours with a random identification number that is generated by the device every twenty-four hours. The GPS Information cannot be associated with a particular customer or device.

The collected GPS Information is stored in a database accessible only by Apple.

D. iAd Network

On July 1, 2010, Apple launched the iAd mobile advertising network for iPhone and iPod touch devices running iOS 4. The iAd network offers a dynamic way to incorporate and access advertising within applications. Customers can receive advertising that relates to their interests ("interest-based advertising") and/or their location ("location-based advertising"). For example, a customer who purchased an action movie on iTunes may receive advertising regarding a new action movie being released in the theaters or on DVD. A customer searching for nearby restaurants may receive advertising for stores in the area.

As specified in the updated Policy and the iPhone 4 and iPod touch SLAs, customers may opt out of interest-based advertising by visiting the following site from their mobile device: https://oo.apple.com. Customers also may opt out of location-based advertising by toggling the device's location-based service capabilities to "Off."[10]

For customers who do not toggle location-based service capabilities to "Off," Apple collects information about the device's location (latitude/longitude coordinates) when an ad request is made. This information is transmitted securely to the Apple iAd server via a cellular network connection or Wi-Fi Internet connection. The latitude/longitude coordinates are converted immediately by the server to a five-digit zip code. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Apple does not share any interest-based or location-based information about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive overly repetitive and/or duplicative ads and for administrative purposes.

---

searching for a cellular network. This information is sent anonymously to Apple to assist the device with locating an available channel. Apple does not retain this GPS Information in its database.

[10] A customer who opts out of interest-based and location-based advertising may still receive ads. The ads, however, will likely be less relevant to the customer because they will not be based on either interests or location. The customer also may receive interest-based or location-based ads from networks other than the iAd network.

In some cases, an advertiser may want to provide more specific information based on a device's actual location. For example, a retailer may want its ad to include the approximate distance to nearby stores. A dialogue box will appear stating: "iAd would like to use your current location." The customer is presented with two options: "Don't Allow" or "OK." If a customer clicks "Don't Allow," no additional location information is transmitted. If the customer clicks "OK," Apple uses the latitude/longitude coordinates to provide the ad application with more specific location information—the information is not provided to the advertiser.

III. THIRD-PARTY APPLICATIONS

A. Overview

In July 2008, Apple launched the App Store where customers may shop for and acquire applications offered by third-party developers for the iPhone, iPad, and iPod touch. Currently the App Store includes more than 200,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation, and social networking. Each application includes a description prepared by the developer regarding, among other things, what the application does, when it was posted, and, if applicable, what information the application may collect from the customer.

Any customer with an iTunes account may purchase and download applications from the App Store. Developers do not receive any personal information about customers from Apple when applications are purchased. Only Apple has access to that information.

B. Third-Party Developers

Third-party application developers must register as an "Apple Developer" by paying a fee and signing the iPhone Developer Agreement (the "IDA") and the Program License Agreement (the "PLA"). Registered Apple Developers gain access to the software development kit ("SDK") and other technical resources necessary to develop applications for mobile devices.

The current PLA contains several provisions governing the collection and use of location-based information, including the following:

- Developers may collect, use, or disclose to a third party location-based information only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the application (PLA § 3.3.9);

- Developers must provide information to their customers regarding the use and disclosure of location-based information (*e.g.*, a description on the App Store or adding a link to the applicable privacy policy) (PLA § 3.3.10);

- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access (*id.*);

- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information (PLA § 3.3.11);

- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers (PLA § 3.3.12); and

- Applications must not disable, override, or otherwise interfere with Apple-implemented alerts, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use (PLA § 3.3.14).

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate the PLA if a developer fails to comply with any of these provisions. (PLA § 12.2.)

Apple reviews all applications before adding them to the App Store to ensure, for example, that they run properly and do not contain malicious code. Apple, however, does not monitor applications after they are listed in the App Store, unless issues or problems arise.

IV. RESPONSES

The following responses represent the current state of our knowledge based on our investigation to date. Our investigation is ongoing, however, and we may continue to discover information responsive to your letter. I will update our responses, as needed, if we locate other responsive materials or information.

1. **Which specific Apple products are being used by Apple to collect geographic location data?**

The iPhone 3G, iPhone 3GS, iPhone 4, iPad Wi-Fi + 3G, and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, iPod touch, Mac computers running Snow Leopard, and Windows or Mac computers running Safari 5.

2. **When did Apple begin collecting this location data, and how often is data collected from a given consumer?**

Apple first began offering location-based service in January of 2008 and began collecting Wi-Fi Access Point Information at that time.

As described above, collection of location data varies greatly based on the services requested by each customer. Location data will not be collected at all from those users who have location services turned off.

3. **Does Apple collect this location data from all consumers using Apple products? If the answer is no, please explain which consumers Apple is**

collecting information from and the reasons that these consumers were chosen for monitoring?

Apple collects anonymous Wi-Fi Access Point, Cell Tower and GPS Information from devices that have location services turned on, have explicitly authorized apps to use their location, and are actively running one of the apps. Anonymous Wi-Fi Access Point Information and GPS coordinates may also be collected when an iPhone is using GPS to search for a cellular network. Diagnostic location data is only collected from users who have expressly agreed to send this information to Apple. Device location data (by zip code only) is collected from users who participate in the iAd network.

4. **How many consumers are subject to this collection of location data?**

Please see our answer to question #3 above.

5. **What internal procedures are in place to ensure that any location data is stored "anonymously in a form that does not personally identify" individual consumers?**

When a customer's device sends Wi-Fi, cell tower, GPS or diagnostic location data to Apple it does not include any information identifying the particular device or user.

In the case of the iAd network, latitude and longitude coordinates are collected and immediately converted to a five-digit zip code. Latitude and longitude coordinates are not kept or otherwise associated with an individual. Apple's iAd server does associate the five-digit zip code with a device identifier for the purpose of serving a location-relevant ad. Apple does not share any location data about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive duplicative ads and for administrative purposes. Apple intends to retain the zip code information it has collected for six months to administer and improve the iAd network. After six months, the information may be aggregated for administrative purposes.

6. **Please explain in detail why Apple decided to begin collecting location data at this time, and how it intends to use the data.**

Please see our answer to question #2 above regarding when we began collecting relevant information. Apple collects location data for only one purpose—to enhance and improve the services we can offer to our customers.

7. **Is Apple sharing consumer location information collected through iPhones and iPads with AT&T or other telecommunications carriers?**

No.

8. **Who are the unspecified "partners and licensees" with which Apple shares this location data, and what are the terms and conditions of such information sharing? How does this comply with the requirements of Section 222 of the Communications Act, which mandates that no consumer location information be shared without the explicit prior consent of the consumer?**

The "licensees" referred to above are our software application developers. Apple shares location data with an application developer only after a user has given express consent to the sharing.

"Partners" refers to two external partners who maintain databases of known locations for cell towers and Wi-Fi access points. Earlier versions of the iPhone software rely on these databases for Wi-Fi access point and cell tower locations. For devices running that earlier software, Apple shares anonymous, non-device identifying location information with these external partners to obtain better location results for our users.

9. **Does Apple believe that legal boilerplate in a general information policy, which the consumer must agree to in order to download applications or updates, is consistent with the intent of Section 222, and sufficient to inform the consumer that the consumer's location may be disclosed to other parties? Has Apple or its legal counsel conducted an analysis of this issue? If yes, please provide a copy. If not, why not?**

While Apple is not a telecommunications carrier or service provider subject to Section 222, we believe the privacy protections described in detail in this letter are consistent with the intent of Section 222.

Apple is committed to giving our customers clear notice and control over their information, and we believe our products do this in a simple and elegant way. We share your concerns about the collection and misuse of location data, and appreciate this opportunity to explain our policies and procedures.

Sincerely,

Bruce Sewell
General Counsel and Senior Vice President of
Legal and Government Affairs