



Het wordt persoonlijk.

Hoe misbruik van het interoperabiliteitsmandaat van de DMA jouw privégegevens kan blootleggen

December 2024 | vertaling > NL door DeepL

Bij Apple stellen we ontwikkelaars graag in staat om geweldige apps te bouwen voor onze gebruikers.

Als het op nieuwe producten en functies aankomt, is de aanpak van Apple altijd hetzelfde. We innoveren om ervaringen te creëren die onze gebruikers geweldig vinden. En we doen er alles aan om hun privacy en veiligheid te beschermen. Daarnaast bieden we onze ontwikkelaars een steeds groter wordende verzameling tools, technologieën en hulpmiddelen waarmee ze geweldige apps kunnen bouwen op onze producten. waarmee ze fantastische apps kunnen maken op onze apparaten. Apple heeft miljarden dollars geïnvesteerd in de ontwikkeling van geweldige producten en functies die ontwikkelaars hebben gebruikt om bijzondere dingen te creëren, waaronder zeer succesvolle eigen bedrijven.

Apple heeft meer dan

250,000

application programming interfaces of API's gemaakt. API's zijn tools waarmee ontwikkelaars gebruik kunnen maken van de ongelofelijke functies die we hebben gebouwd.

Deze toewijding aan onze ontwikkelaars is een fundamenteel onderdeel van het DNA van Apple. We hebben baanbrekend werk verricht, zowel voor ontwikkelaars als voor onszelf, om geweldige gebruikerservaringen mogelijk te maken zonder dat enig bedrijf, waaronder Apple, toegang heeft tot de privégegevens van gebruikers. Dit vormt de basis voor het vertrouwen van gebruikers en maakt het succes mogelijk voor iedereen: gebruikers, ontwikkelaars en Apple.

Apple streeft naar succes voor ontwikkelaars door middel van interoperabiliteit die de privacy beschermt

Onze gebruikers verdienen een volledig en transparant inzicht in waarom een ontwikkelaar toegang wil tot belangrijke onderdelen van hun apparaten, wat die ontwikkelaar ermee gaat doen en wanneer dat gebeurt.



Microfoon

Toen we ontwikkelaars toegang gaven tot de microfoon op iPhone, zodat ze konden luisteren naar wat een gebruiker zei en deed, hielden we de gebruiker de controle.

Ontwikkelaars moeten gebruikers toestemming vragen voor toegang tot de microfoon en ze moeten gebruikers laten weten wanneer ze die toegang gebruiken om geluid op te nemen.



Touch ID

Touch ID werd in 2013 geïntroduceerd en is de eerste populaire en gebruiksvriendelijke biometrische toegangstechnologie voor smartphones. Bij gebruik bewaart Apple de vingerafdrukgegevens van gebruikers in de Secure Enclave van de iPhone, waar zelfs Apple geen toegang toe heeft. In 2014 werd de Touch ID API voor ontwikkelaars uitgebracht, zodat ontwikkelaars van apps voor banken, games en meer deze technologie kunnen gebruiken zonder dat de veiligheid en privacy van de gebruiker in het geding komen.

Maar we zien nu concrete voorbeelden van hoe **een nieuwe benadering van interoperabiliteit in de EU gebruikers in gevaar zou brengen**, door hen te verplichten hun apparaten - en hun meest gevoelige gegevens - open te stellen voor bedrijven die hun privacy hebben geschonden.



De magische ervaringen die mensen zo waarderen aan Apple producten zijn mogelijk dankzij de tijd, het talent en het kapitaal dat het bedrijf besteedt aan het maken van producten die direct werken.

Deze processen zullen de innovatie schaden - bedrijven zouden met elkaar moeten kunnen concurreren om hun eigen producten op nieuwe manieren te laten samenwerken waar gebruikers baat bij hebben, zonder hun ideeën weg te geven aan concurrenten. Apple is het enige bedrijf dat gedwongen wordt om zijn innovaties op deze manier met iedereen te delen, ook met bedrijven die het niet eens zijn met de privacy van gebruikers.

Interoperabiliteitsrisico's

Eerder dit jaar ging de Digital Markets Act van start, waarmee het concept van "interoperabiliteit" in de wet werd vastgelegd. Het basisidee is dat ontwikkelaars toegang moeten hebben tot dezelfde tools in iOS en iPadOS als Apple, om een gelijk speelveld te garanderen. Apple heeft altijd in dat gelijke speelveld geloofd. We blijven mogelijkheden voor interoperabiliteit creëren, maar het blijft ongelooflijk belangrijk om dat te doen op een manier die goed is voor onze gebruikers. **Daarom denken we er elke keer dat we ontwikkelaars toegang geven tot functionaliteiten goed over na hoe we dit kunnen doen op een manier die gebruikers blijft beschermen.** We kennen allemaal de risico's. Zonder de juiste bescherming kan het verlenen van toegang aan derden tot delen van de apparaten van gebruikers slechte actoren de mogelijkheid bieden om hun persoonlijke gegevens te stelen of openbaar te maken.

Nu apparaten steeds persoonlijker worden, is het uiterst belangrijk om de bescherming van gebruikers centraal te stellen bij alles wat we doen. Apple doet veel moeite om software te ontwikkelen die de privacy en veiligheid van gebruikers beschermt. We maken ons zorgen dat sommige bedrijven - die gegevens gebruiken die niet voldoen aan de hoge normen van gegevensbeschermingswetgeving die door de EU worden gehanteerd en door Apple worden gesteund - zouden kunnen proberen de interoperabiliteitsbepalingen van de DMA te misbruiken om toegang te krijgen tot gevoelige gebruikersgegevens.

Gegevensbeluste bedrijven over de hele wereld kunnen interoperabiliteit als wapen gebruiken

In ons streven om te voldoen aan de DMA, beoordelen we elk verzoek om interoperabiliteit dat we ontvangen zorgvuldig. Om een voorbeeld te geven van onze bezorgdheid: Meta heeft 15 verzoeken ingediend (en er komen er nog steeds bij) voor mogelijk verstrekking van toegang tot Apple's technologie die, als ze worden ingewilligd zoals gevraagd, de bescherming van persoonlijke gegevens die onze gebruikers van hun apparaten zijn gaan verwachten, zou verminderen.

Enkele van de gevoelige technologieën waarvoor Meta toegang heeft gevraagd

Geen enkel bedrijf heeft meer verzoeken tot interoperabiliteit ingediend bij Apple dan Meta. In veel gevallen probeert Meta functionaliteit te veranderen op een manier die zorgen oproept over de privacy en veiligheid van gebruikers, en die volledig los lijkt te staan van het daadwerkelijke gebruik van externe Meta-apparaten, zoals de Meta-smartbril en Meta Quests.



AirPlay



App-intenties



Dienst Meldingscentrum van Apple



CarPlay



Connectiviteit met alle Apple apparaten van een gebruiker



Continuïteit camera



Apparaten verbonden met Bluetooth



iPhone spiegelen



Berichten



Wi-Fi-netwerken en eigenschappen

Derde partijen hebben mogelijk niet dezelfde toewijding om de gebruiker controle te geven over hun apparaat als Apple.

Als Apple al deze verzoeken zou moeten inwilligen, zouden **Facebook, Instagram en WhatsApp** Meta in staat stellen al hun berichten en e-mails op het apparaat van een gebruiker te lezen, elk telefoongesprek dat ze voeren of ontvangen in te zien, elke app die ze gebruiken te volgen, al hun foto's te scannen, hun bestanden en agenda-afspraken te bekijken, al hun wachtwoorden te loggen en nog veel meer. **Dit zijn gegevens die Apple zelf niet toegankelijk wil maken om gebruikers zo goed mogelijk te beschermen.**

Apple verzamelt alleen de persoonlijke gegevens die strikt noodzakelijk zijn om een product of dienst te leveren, we geven de gebruiker controle door toestemming te vragen voordat apps toegang krijgen tot gevoelige gegevens en we geven duidelijke indicaties wanneer apps toegang krijgen tot bepaalde gevoelige functies zoals de microfoon, camera en de locatie van de gebruiker. We verwerken gegevens waar mogelijk op het apparaat in plaats van ze naar Apple servers te sturen, om de privacy van gebruikers te beschermen en het verzamelen van gegevens tot een minimum te beperken. Derde partijen hebben mogelijk niet dezelfde toewijding om de gebruiker de controle te laten houden over hun apparaat als Apple en geven er mogelijk de voorkeur aan om gebruikersgegevens naar hun servers te sturen - waar ze de privégegevens van een individu kunnen combineren, profileren en te gelde maken.

De General Data Protection Regulation (GDPR), die Apple altijd heeft gesteund, heeft een reeks strenge privacyregels opgesteld waaraan alle bedrijven moeten voldoen. De DMA was niet bedoeld om deze regels te omzeilen. Maar het eindresultaat zou kunnen zijn dat bedrijven als Meta - dat keer op keer door toezichthouders is beboet voor privacyschendingen - onbeperkte toegang krijgen tot de apparaten van gebruikers en hun meest persoonlijke gegevens. Als Apple gedwongen wordt om toegang te verlenen tot gevoelige technologieën die het niet kan beschermen, zijn de veiligheidsrisico's aanzienlijk en vrijwel onmogelijk te beperken.



Berichten

Meta wil toegang krijgen tot de SMS- en iMessage-mogelijkheden van gebruikers om zelf berichten te versturen en te lezen. Los daarvan wil Meta ook toegang tot hun berichtengeschiedenis. Toegang tot privécommunicatie moet volledig onder controle van de gebruikers blijven.



AirPlay

Apple ondersteunt al jaren dat apps content kunnen versturen via AirPlay. Meta vraagt om directe toegang tot de tv's en slimme luidsprekers van gebruikers, wat een nieuwe klasse van privacy- en beveiligingsproblemen creëert, terwijl Meta gegevens krijgt over de huizen van gebruikers.



App-intenties

Meta wil toegang tot alle gegevens die door andere apps worden verstrekt voor App Intents, een nieuw raamwerk voor het beheer van de manier waarop gebruikers omgaan met de apps en functies op hun apparaten. Dergelijke toegang zou Meta mogelijk de mogelijkheid geven om het apparaat van een gebruiker volledig te controleren.



CarPlay

Meta wil toegang tot de CarPlay-functionaliteit, zodat het iOS-apps kan wekken en extra content kan projecteren op apparaten van gebruikers. Dit ontnemen van controle aan gebruikers zou hun keuzes kunnen ondermijnen.

Als een gebruiker Siri bijvoorbeeld vraagt om het laatste bericht dat hij via WhatsApp heeft ontvangen hardop voor te lezen, kunnen Meta of andere derde partijen indirect toegang krijgen tot de inhoud van het bericht. Niemand kan de volledige risico's daarvan overzien.

Apple's streven naar interoperabiliteit

We werken er hard aan om alle verzoeken te beoordelen en waar mogelijk uit te voeren, rekening houdend met de noodzaak om de privacy en veiligheid op het platform te beschermen. Zelfs als de verzoeken ernstige risico's met zich meebrengen, zoals we hier hebben laten zien, onderzoeken we verbeteringen aan ons platform die rijkere ervaringen mogelijk maken, terwijl we gevoelige gebruikersgegevens blijven beschermen en de beveiliging van apparaten handhaven. We streven ernaar om alle verzoeken tijdig te evalueren en te beantwoorden, zodat de integriteit van het platform voor alle ontwikkelaars behouden blijft en gevoelige gebruikersgegevens worden beschermd.

Het proces van Apple voor het aanvragen van interoperabiliteit

Aanvraag indienen

Ontwikkelaars van apps in de EU kunnen een verzoek indienen voor interoperabiliteit met hardware- en softwarefuncties die zijn ingebouwd in iOS, iPadOS, iPhone en/of iPad.

Eerste beoordeling

Apple beoordeelt in eerste instantie of het verzoek binnen artikel 6, lid 7, van de DMA valt.

Voorlopig projectplan

Apple begint met het ontwerpen van een oplossing voor effectieve interoperabiliteit met de gevraagde functie.

Ontwikkeling en vrijgave

Voor zover een effectieve oplossing haalbaar en geschikt is onder de DMA, zal Apple de oplossing ontwikkelen.

Apple beoordeelt elk verzoek en houdt ontwikkelaars op de hoogte van de voortgang nadat een verzoek is ingediend. Als Apple op enig moment in het proces vaststelt dat het niet haalbaar is om een effectieve interoperabiliteitsoplossing te ontwerpen of dat het niet gepast is om dit te doen in het kader van de DMA, delen we dat mee aan de ontwikkelaar.



De hoge normen die Apple hanteert op het gebied van **privacy** en **beveiliging** vormen het onderscheidend vermogen van Apple.

Onze gebruikers zijn ervan afhankelijk. We willen dat zowel gebruikers als ontwikkelaars veilig kunnen profiteren van de geweldige functies en mogelijkheden van iPhone.

We zullen nooit afstand doen van onze fundamentele toewijding aan de privacy en veiligheid van onze gebruikers. We vertrouwen erop dat de EC zal proberen de interoperabiliteitseisen te implementeren op een manier die de GDPR respecteert.