



داده‌های جمع‌آوری شده توسط این سرویس‌ها گردآوری، تجمیع و پردازش شده و به اطلاعات بازاریابی هوشمندی تبدیل می‌شود که نتیجه آن یک صنعت عظیم با گردش مالی ۲۲۷ میلیارد دلار در سال است. راهکار اپل برای مقابله با این وضعیت و حفاظت از اطلاعات کاربران، تعریف سازوکاری به نام ATT یا شفافیت ردگیری توسط اپلیکیشن‌هاست. همان‌طور که گفتیم این قابلیت از یک سال پیش در آی‌اواس تعبیه شده بود، اما از بهار امسال همه توسعه‌دهندگان از جمله خود اپل موظف به فعال‌سازی آن خواهند بود.

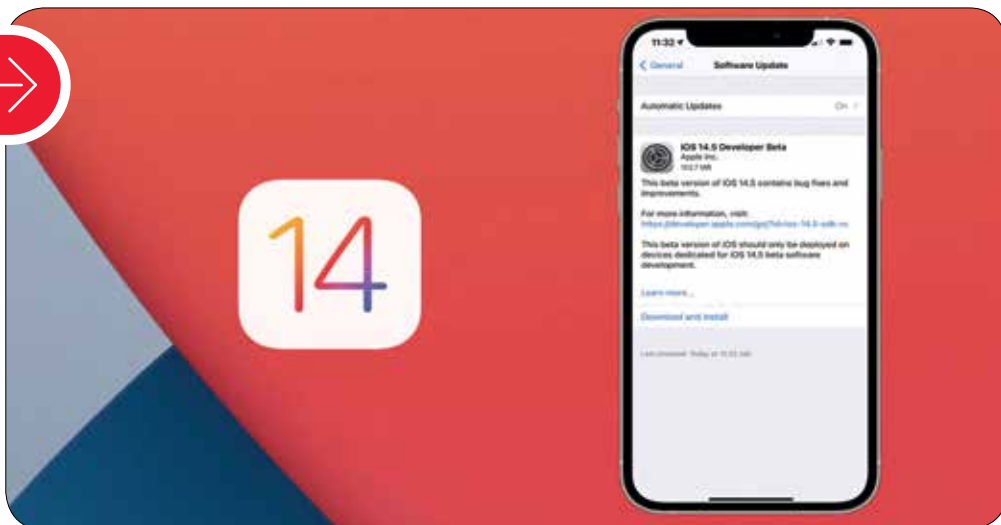
به این ترتیب، می‌توانید ببینید کدام اپلیکیشن‌ها درخواست دنبال کردن شما در دیگر برنامه‌ها یا وبسایت‌ها را دارند و می‌توانید بسته به نظر خود به آنها اجازه این کار را بدهید یا ندهید. البته در صورتی که بخواهید به سرویس‌های موردنظرتان اجازه دنبال کردن خود را بدهید، می‌توانید این کار را بکنید. هرچند دیگر این تصمیم فردی شماست و کسی ناخواسته اقدام به جمع‌آوری اطلاعات شما نخواهد کرد. نکته دیگر این است که با ندادن اجازه ردگیری شما در اینترنت، مشکلی در استفاده از خود برنامه نخواهید داشت و اختیار کامل حریم خصوصی‌تان در دست خودتان است. برای فعال‌سازی این قابلیت می‌توانید وارد قسمت تنظیمات و سپس Privacy شوید. حال در قسمت Tracking گزینه‌ای به نام Allow Apps to Request to Track را پیدا کرده و آن را فعال کنید. البته فعال‌سازی این گزینه فعلا هیچ عملکردی ندارد، اما با شروع الزام توسعه‌دهندگان به درخواست اجازه از کاربران، می‌توانید از مزایای آن استفاده کنید.

➤ به خواندن برجسب عادت کنید

یکی دیگر از اقدامات اپل برای بهبود حریم خصوصی کاربران، بهبود توانایی آنها در تشخیص میزان و کیفیت حفظ حریم خصوصی در اپلیکیشن‌ها بوده است. این شرکت تمام توسعه‌دهندگان نرم‌افزارهای خود را ملزم به ارائه یک خلاصه سریع و قابل درک از سیاست‌های حفظ حریم خصوصی به کاربران کرده است. بنابراین با مراجعه به قسمت App Privacy در فروشگاه App Store می‌توانید اطلاعات مرتبط با حفظ حریم خصوصی خود توسط اپلیکیشن موردنظر را در یک قالب استانداردسازی شده و همه فهم مشاهده کنید. این برجسب‌ها که از برجسب‌های اطلاعات تغذیه‌ای موجود روی بسته‌بندی مواد غذایی الهام گرفته شده‌اند، در یک نگاه به شما نشان می‌دهد اپلیکیشنی که قصد دریافت یا خرید آن را دارید با اطلاعات شما چه کار می‌کند. این اطلاعات حتی جزئیاتی از قبیل این‌که آیا اطلاعات ثبت شده توسط اپلیکیشن برای ردگیری آنها استفاده خواهد شد یا نه را هم شامل می‌شود. بنابراین بهترین کار این است که درست مثل خرید مواد غذایی، خودتان را به خواندن این برجسب‌ها عادت دهید. با این کار، هم بهتر می‌توانید از حریم خصوصی خود محافظت کنید، هم بیشتر با اپلیکیشن‌ها و توسعه‌دهندگانی که احترامی برای آن قائل نیستند آشنا می‌شوید.



اپل یک سال به توسعه‌دهندگان و شرکای خود فرصت داده بود تا خود را برای این تغییرات آماده کنند



قابلیت‌های جدیدی به زودی در آی‌اواس فعال می‌شوند تا حریم خصوصی ایمن‌تری داشته باشید

اختیار کامل



خشایار مریدیپور

روزنامه‌نگار فناوری

اپل به تازگی اعلام کرده در بهر روزرسانی بعدی آی‌اواس که قرار است از بهار امسال عرضه شود، برخی قابلیت‌های کلیدی مرتبط با حفظ حریم خصوصی کاربران را عملیاتی خواهد کرد. البته این قابلیت‌ها جدید نیستند و در واقع هم‌زمان با عرضه نسخه ۱۴ سیستم عامل آی‌اواس و آپید اواس رونمایی شده بودند. هرچند، اپل ناچار شد مدتی به توسعه‌دهندگان و دیگر شرکای خود فرصت دهد تا خود را با این تغییرات سازگار کنند. حتی این ویژگی‌ها در آخرین نسخه بتای سیستم عامل‌های اپل هم دیده شده بود، اما کماکان به نسخه نهایی که همین اواخر عرضه شد، اضافه نشده است. طبق اعلامیه اپل در روز «حفاظت از اطلاعات فردی»، این ویژگی‌های جدید از اوایل بهار سال بعد فعال شده و تغییر چشمگیری در میزان محافظت از اطلاعات خصوصی کاربران آیفون و آپید ایجاد خواهد کرد. به همین بهانه می‌خواهیم شما را بیشتر با این قابلیت‌ها، نحوه فعال‌سازی آنها و تأثیری که بروند استفاده کاربران از آیفون و آپید خواهند گذاشت، آشنا کنیم.

➤ به سافاری اطمینان کنید

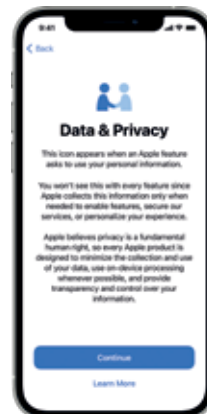
مرورگر اختصاصی اپل یعنی سافاری به داشتن قابلیت‌های مناسب برای حفظ حریم خصوصی کاربران شهره است. اما به نظر می‌رسد قرار است این سختگیری در جلوگیری از نشر اطلاعات کاربران ابعاد جدیدی پیدا کند. یکی از قابلیت‌های مرورگر سافاری، امکان دریافت هشدار درباره وبسایت‌ها و آدرس‌های URL مشکوک است. برای این کار باید وارد سافاری شده و در قسمت تنظیمات گزینه Fraudulent Website Warning را فعال کنید. به این ترتیب بهتر می‌توانید از خود در برابر خطرات استفاده از سرویس‌ها و وبسایت‌های احتمالا مخرب محافظت کنید.

اپل و مرورگر آن یعنی سافاری تا همین اواخر از سرویس پایگاه داده وبسایت‌های مشکوک گوگل برای شناسایی آدرس‌های اینترنتی مشکل‌دار و هشدار به کاربران استفاده می‌کردند. در این سیستم، اپل نسخه کوتاه شده‌ای از آدرس اینترنتی درخواستی کاربر را برای گوگل ارسال می‌کرد و آن را با فهرست وبسایت‌های مشکل‌دار این شرکت تطبیق می‌داد. از آنجا که آدرس به صورت خلاصه شده به گوگل ارسال می‌شود، امکان شناسایی

آدرس موردنظر برای سایت گوگل وجود نداشت. هرچند این شرکت کماکان می‌توانست به آدرس IP کاربران سافاری دسترسی داشته باشد و از این اطلاعات برای ارسال تبلیغات هدفمند استفاده کند. تصاویری که از عملکرد سافاری در نسخه بتای جدید منتشر شده اما چیز دیگری را نشان می‌دهد. در بهر روزرسانی جدید، اپل ترافیک مرتبط با درخواست‌های شناسایی وبسایت‌های مشکوک توسط گوگل را با پراکسی‌های داخلی خود انجام می‌دهد. این باعث می‌شود که یک لایه امنیتی دیگر برای اطلاعات فردی شما ایجاد شود. این مساله می‌تواند تأثیر جدی بر قابلیت گوگل در ارسال تبلیغات هدفمند و کسب درآمد از این راه داشته باشد، اما در نحوه استفاده شما از این مرورگر هیچ تغییری ایجاد نخواهد شد. همچنین پیشنهاد می‌کنیم با مراجعه به قسمت Privacy & Security در قسمت تنظیمات مرورگر سافاری، قابلیت Prevent Cross-Site Tracking را هم غیرفعال کنید تا هرچه بیشتر امکان ردیابی خود توسط سایت‌ها و سرویس‌های مختلف را کاهش دهید.

➤ ردتان را گم کنید

وقتی از یک اپلیکیشن روی آیفون یا آپید خود استفاده می‌کنید، ممکن است جزئیات کارکرد شما با گوشی در اپلیکیشن‌های دیگر یا اینترنت هم ردگیری شود. هدف از این کار، مسلمانمایش تبلیغات مرتبط و کسب درآمد است. ولی در این بین، به حریم خصوصی کاربران می‌تواند تعرض جدی شود. این چیزی بود که اپل در اعلامیه روز حفاظت از اطلاعات فردی با گزارشی به نام «یک روز در زندگی داده‌های شما» به کاربران نشان داد. طبق اعلام خود اپل هر اپلیکیشن به طور میانگین ۶ «ردیاب» در خود دارد. همان‌طور که گفتیم، کار این ردیاب‌ها گردآوری هرچه بیشتر اطلاعات درباره کاربران است.



به زودی در تمام اپلیکیشن‌های آی‌اواس برای دنبال کردن نحوه استفاده کاربر از برنامه یا وبسایت‌ها اجازه او ضروری خواهد بود. این قابلیت کلیدی آژانس‌های تبلیغاتی را از جزئیات نحوه استفاده کاربران از اینترنت محروم خواهد کرد