

Nový plán společnosti Google vás sledovat na internetu

 infokuryr.cz/n/2024/10/27/novy-plan-spolecnosti-google-vas-sledovat-na-internetu

kuryr

27. října 2024

Cookies třetích stran jsou v prohlížeči Google Chrome (téměř) mrtvé – ať žije cookie třetí strany?

Zda je to pravda – ve skutečnosti – je otázka, kterou vyvolává nedávno představená funkce společnosti Google s názvem Related Website Sets (RWS) (přejmenovaná z First-Party Sets).

„Způsob, jak může společnost deklarovat vztahy mezi weby,“ tak to rád shrnuje Google.

Konkrétněji definuje skupinu „souvisejících webů“, které sdílejí „důvěryhodný obsah“.

Představte si, že máte sadu klíčů pro různé místnosti v domě – každá místnost představuje jiný web vlastněný stejnou společností (např. YouTube, Gmail a Mapy Google). S RWS Google navrhuje scénář, kdy jakmile odemknete místnost, ostatní místnosti vás poznají a automaticky se otevřou, aniž byste znovu potřebovali klíč. Tento „objev“ technicky znamená, jak webové stránky identifikují a sledují uživatele v různých službách od stejné společnosti.

Když navštívíte webovou stránku, malé kousky dat nazývané soubory cookie pomáhají webu zapamatovat si informace o vaší návštěvě. Dříve nebylo možné soubory cookie z jedné webové stránky sdílet s jinou, pokud tyto dvě webové stránky výslovně neuzavřely partnerství (představte si, že byste potřebovali zvláštní dohodu o použití stejného klíče pro různé místnosti vlastněné různými lidmi). RWS to mění tím, že umožňuje skupině webových stránek vlastněných stejnou společností automaticky vzájemně rozpoznávat soubory cookie.

Zastánci RWS tvrdí, že zlepšuje uživatelskou zkušenost tím, že umožňuje bezproblémovou interakci mezi různými službami. Pokud jste například přihlášení do Gmailu, můžete snadno přistupovat na YouTube nebo Mapy Google, aniž byste se museli znovu přihlašovat. Společnost tvrdí, že jde o pohodlí a udržení uživatelsky přívětivých služeb na konkurenčním trhu.

Názory kritiků:

Kritici však vidí RWS jako sofistikovaný nástroj pro hlubší sledování a profilování uživatelů. Hlavním problémem je, že sdílením souborů cookie na více webových stránkách by Google mohl potenciálně sledovat uživatele šířeji napříč různými službami a shromažďovat údaje o jejich aktivitách způsobem, který uživatelé neočekávají nebo si toho nejsou vědomi.

Vylepšené možnosti sledování: S RWS, jakmile interagujete s webem ve skupině, ostatní weby v této skupině mají přístup k těmto informacím, což může vést k podrobnějšímu sledování vašeho online chování. Například to, co vyhledáváte na Googlu, může ovlivnit to, co vidíte na YouTube, bez jasných hranic.

Rozmazané hranice souhlasu: Pro uživatele je obtížnější ovládat svá nastavení ochrany osobních údajů, když jsou jejich data automaticky distribuována na více webových stránek. To může vést k rozmazání hranic toho, co uživatelé sdílejí, a ztížit jim pochopení, kdo má jejich data a jak jsou využívána.

Potenciál pro šíření dat: Možnost přístupu více webových stránek ke stejným souborům cookie by mohla vést k šíření osobních údajů na různých platformách, což by zvýšilo riziko narušení dat nebo neoprávněné sdílení dat.

Brave Software, jedna z alternativ Google Chrome zaměřená na ochranu soukromí a zabezpečení a výrobce prohlížeče Brave, se společně s výzkumníky z University of St. Andrews, Imperial College

London a Hong Kong University of Science & Technology rozhodli bližší pohled prozkoumat .

Studie zkoumala , jaké škody a rizika může RWS přinést, pokud a jak soubory cookie třetích stran (které mají být vyřazeny zdlouhavým procesem) se „vrací“ v jiné podobě a poskytují výhody ochrany údajů, z nichž by jinak měli prospěch uživatelé. zničit.

Google říká, že cílem RWS je znovu vytvořit „zážitky“, které dříve umožňovaly soubory cookie třetích stran, ale tentokrát s ohledem na „vylepšené soukromí“. A Google je jednoznačný – „zkušenosti“ jsou nezbytné a je třeba je znovu vytvořit.

„Související sady webových stránek představují způsob, jak může společnost deklarovat vztahy mezi webovými stránkami, takže prohlížeče umožňují omezený přístup k souborům cookie třetích stran pro konkrétní účely,“ vysvětluje Google na svých webových stránkách zaměřených na vývojáře.

Chrome pak tyto informace použije k „rozhodnutí, kdy webu povolit nebo zakázat přístup k jeho souborům cookie, když je v kontextu třetí strany“.

Jedna věc se zdá jasná: Google odkládá odstranění souborů cookie třetích stran, zatímco vyvíjí náhradu. Nabízí se pouze otázka, zda tato náhrada bude vylepšením nebo jen fíkovým listem.

Studie chování RWS, shrnutá na webu Brave, tvrdí, že navzdory pozitivnímu zobrazení této funkce Googlem je RWS na újmu soukromí, protože „navrací některé výhody ochrany soukromí vyplývající z eliminace souborů cookie třetích stran“.

Konec souborů cookie třetích stran

Soubory cookie třetích stran jsou již léta páteří online reklamy. Sledují aktivity uživatelů na různých webech a poskytují personalizovanou reklamu. Tyto soubory cookie jsou nastaveny jinými doménami než doménami, které přímo navštěvujete, a

umožňují inzerentům sledovat vaše zvyky při procházení webu. Tato praxe však vyvolala značné obavy o soukromí a vedla k přísnějším regulacím, jako je GDPR v Evropě a CCPA v Kalifornii.

V reakci na tyto obavy a měnící se postoje spotřebitelů k soukromí společnost Google oznámila, že ve svém prohlížeči Chrome odstraní soubory cookie třetích stran. Toto rozhodnutí bylo také podníceno podobnými kroky jiných prohlížečů, jako je Firefox a Safari, které již ve výchozím nastavení začaly blokovat soubory cookie třetích stran.

RWS umožňuje sbírce souvisejících webových stránek vzájemně rozpoznávat soubory cookie. To znamená, že i když jsou soubory cookie třetích stran blokovány, řada webových stránek vlastněných stejnými vlastníky může mezi sebou stále sdílet údaje o sledování.

Kromě toho, důvody uváděné společností Google pro zavedení této funkce – jako jakési oznámení o transparentnosti pro uživatele Chrome, že organizace provozuje různé webové stránky – jsou do značné míry zbytečné, když uvážíte, kolik uživatelů jí bude skutečně věnovat pozornost.

Jak RWS a její „organizace, která provozuje různé webové stránky“ ve skutečnosti funguje, je vysvětleno na příkladu Google, který jej používá ke sledování videí, která uživatel sleduje na YouTube (bez ohledu na to, zda je přihlášen ke svému účtu či nikoli). odkaz na celý jeho účet Google. Totéž platí například pro Facebook a Instagram, protože oba patří společnosti Meta.

Proč by si ale uživatel měl myslet, že je na tom z hlediska ochrany soukromí lépe než nyní, když je sledují soubory cookie třetích stran a vysávají život z jeho osobních údajů, aby nakrmily reklamní průmysl?

Proč ta starost?

1. Pokračování ve sledování: Zatímco odstranění souborů cookie třetích stran bylo považováno za vítězství zastánců soukromí, zavedení RWS se může zdát jako krok zpět. V podstatě to Googlu umožňuje pokračovat ve sledování uživatelů napříč širokým spektrem služeb a vytvářet podrobné profily uživatelských preferencí, zájmů a chování.

2. Power Shift: Tento krok lze chápat jako posun v dynamice moci ve prospěch velkých konglomerátů, které vlastní více platforem. Menší podniky a nezávislé webové stránky nebudou mít prospěch z propojených schopností RWS, což může mít za následek méně konkurenční trh, kde mají největší hráči ještě větší výhodu při sledování a cílení uživatelů.

3. Problémy s ochranou soukromí a transparentností: Existují obavy, jak transparentně bude Google s touto novou metodou sledování zacházet. Uživatelé si nemusí být plně vědomi toho, jak jsou jejich informace sdíleny na různých platformách, což by mohlo vést k problémům s efektivní správou nastavení ochrany osobních údajů napříč více službami.

Studie naznačuje, že by si to uživatelé neměli myslet a Google očekávání nejen spravuje, ale v podstatě se je snaží vytvořit.

„Uživatel již očekává, že si oba weby budou vyměňovat informace,“ a proto prohlížeč nemusí blokovat soubory cookie třetích stran, pokud tyto weby patří stejné společnosti,“ shrnuje studie RWS inzerce Google.

Výsledky studie však naznačují, že RWS je další iterací mnoha funkcí vyvinutých a nasazených v minulosti k udržení internetového obchodního modelu Big Tech, konkrétně těch, které jsou přínosem pro reklamní průmysl.

Výzkumníci zjistili, že s RWS dostává „model soukromí“ internetu další zásah, který jej oslabí.

Stejně jako mnoho dalších uživatelsky škodlivých a zbytečně komplikovaných rozhodnutí v zastřešujícím návrhu „ochrany soukromí“ Chrome existuje RWS, aby zajistil, že Chrome bude nadále sloužit především potřebám inzerentů, i když Google (konečně) odstraňuje soubory cookie třetích stran a zrušil jej, “ říká shrnutí studie.

Studie zkoumala, zda (většina) uživatelů internetu skutečně určí, zda spolu webové stránky „souvisejí“, a jak přesné je to podle vlastního seznamu vztahů mezi weby RWS.

„V naší studii se velká většina uživatelů (~73 %) nesprávně rozhodla, zda spolu dva webové stránky alespoň jednou souvisejí, a téměř polovina (~42 %) rozhodnutí učiněných během studie (tj. všechna rozhodnutí všech uživatelů) byla špatně,“ podle výsledků testu.

„Obzvláště znepokojivé je, že v případech, kdy byly oba weby propojeny (podle funkce RWS), 37 % uživatelů předpokládalo, že weby nejsou připojeny, což znamená, že si uživatelé mysleli, že je Chrome ochrání, i když tomu tak nebylo. případ.

Vzhledem k tomu, že základní „premisa“ – nebo argument – pro RWS je považována za „v zásadě nesprávná“, vyvstává další problém: proč by uživatelé měli věřit, že dva webové stránky provozované stejnou organizací jsou z hlediska ochrany soukromí bezpečné? Neměli by, říkají iniciátoři studie.

Dále tvrdí, že jiné prohlížeče jako Brave, Firefox a Safari na rozdíl od Chrome dokážou zastavit sledování uživatelů souvisejícími webovými stránkami (ačkoli by si musely registrovat účty s různými e-maily a „informacemi“ – což znamená, že ani to nebrání Googlu z „propojení“ vašich aktivit napříč různými weby.

A to navzdory skutečnosti, že RWS je prodáván jako „výhodný“ a výrazně pozitivní odklon od cookies třetích stran.

Poznamenává, že existují společnosti, které aktivně pracují na sledování uživatelů na různých webech a obcházejí funkce ochrany osobních údajů v jiných prohlížečích, ale Chrome takové snahy umožňuje, zatímco tyto společnosti pracují na jejich kompenzaci.

Vzhledem k podílu prohlížeče Chrome na trhu je RWS pro web špatnou zprávou, ale je zde také stříbrná čára. Nejen, že nejbližší konkurenti jako Brave, Firefox a Safari odmítli RWS, ale tento „obecný webový návrh“ byl odstraněn z W3C Privacy Community Group – „a už ho nezvažuje žádná skupina ve W3C zaměřená na soukromí“.