

GLOSA

Nahrazení cookies třetích stran ambiciózním systémem Google FLoC

Jakub Klodwig*

Abstrakt: Identifikace koncových zařízení a cílení jejich uživatelů je významně se vyvíjející oblastí, která ovlivňuje každodenní život miliard lidí. Technologické společnosti pod tlakem veřejnosti zakazují používání problematických cookies třetích stran a přicházejí s novými metodami i celými systémy fungování online cílení a behaviorální reklamy. Nové však nemusí znamenat lepší, ale může přinést další či trvalé omezení soukromí, tak jak se o to pokusila společnost Google prostřednictvím systému FLoC (Federated Learning of Cohorts). Tento článek vysvětluje fungování systému FLoC, jímž společnost Google plánovala vyřešit tlak na zákaz cookies třetích stran ve svém dominantním prohlížeči Google Chrome. Propracovaný systém kohort, na kterém společnost Google pracovala řadu let, měl kompletně nahradit cookies třetích stran a současně ještě vylepšit pozici Googlu na trhu online marketingu. Nejen že by totiž Google implementací systému kohort zhoršil postavení ostatních společností nabízejících online behaviorální reklamu, jelikož by musely vycházet z dat, které poskytuje právě systém Google Kohort, ale současně se nový systém kompletně vyloučil regulaci ochrany osobních údajů. Jaké změny, trhliny a rizika měl systém kohort přinést, jak reagovali zástupci odborné veřejnosti, ale i jiní soutěžitelé, a co nakonec způsobilo, že Google svůj nový systém kohort zavrhl, se v článku pokouším mapovat a diskutovat z pohledu ochrany soukromí.

Klíčová slova: soukromí, Google, cookies, online marketing, ePrivacy, FLoC, Google Topics

Úvodem: Aktuální metody identifikace koncových zařízení

Soubory cookies jsou nejrozšířenějším způsobem sledování uživatelů na internetu.¹ Jedná se o malé textové soubory, které navštívený web ukládá² do prohlížečů jeho návštěvníků a tímto způsobem obchází anonymitu klasického http protokolu.³ Soubory cookies

* JUDr. Jakub Klodwig, doktorand, Ústav práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: Jakub.Klodwig@mail.muni.cz. ORCID: <https://orcid.org/0000-0002-9599-2043>. Tento článek vznikl za podpory projektu *Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur* (CZ.02.1.01/0.0/0.0/16_019/0000822).

1 KLODWIG, Jakub. *Pokročilé metody identifikace koncových zařízení*. In: JANOVEC, Michal a kol. (eds). *COFOLA 2020: Sborník příspěvků mladých právníků, doktorandů a právních vědců* [online]. Brno: Masarykova univerzita, 2020, s. 1096 [cit. 16. 4. 2022]. Dostupné z: <<https://www.law.muni.cz/sborniky/cofola/2020/cofola2020.pdf>>; ROESNER, Franziska – KOHNO, Tadayoshi – WETHERALL, David. *Detecting and Defending Against Third-Party Tracking on the Web*. *9th USENIX Symposium on Networked Systems Design and Implementation* [online]. 2012, s. 1. Dostupné z: <<https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf>>.

2 Česká právní úprava, která je implementací čl. 5 odst. 3 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), v § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, vyžaduje pro netechnické či nevyžádané ukládání nebo čtení dat z koncového zařízení předchozí souhlas uživatele. Podrobněji je tato problematika vysvětlena např. v KLODWIG, Jakub. *Ochrana soukromí v kontextu koncových zařízení uživatelů*. Diplomová práce. Brno: Právnická fakulta Masarykovy univerzity, 2019, s. 56.

3 Hypertext Transfer Protocol (http) je klasický bezstavový protokol, který neumí uchovávat stav komunikace a takto postupně identifikovat uživatele, kteří na stránku přistoupí. Přistoupivší uživatel je tak v tomto protokolu bez dalšího vždy nejprve neznámý.

dělíme na cookies prvních stran, které jsou ukládány webem, na kterém se uživatel aktuálně nachází, a cookies třetích stran, které do prohlížečů koncových zařízení ukládají další jiné weby než ten, který si uživatel aktuálně načel. Zatímco cookies prvních stran mohou být ještě považovány za relativně přijatelný nástroj pro zjišťování informací o uživateli, kteří na daný web přistupují, cookies třetích stran jsou odbornou veřejností označovány za jeden z nejintruzivnějších nástrojů pro soukromí koncového uživatele.⁴ Hlavní rozdíl mezi těmito druhy cookies je, že cookies třetích stran fungují *cross-site*, neboli napříč webovými stránkami. To znamená, že když uživatel přistoupí na webovou stránku A, cookies prvních stran budou pouze z této webové stránky A, zatímco cookies třetích stran budou z dalších webových stránek B či C. Uživatel tedy může mít oprávněné očekávání, že jej bude při procházení stránkou sledovat stránka A, na které se nachází, ale nikoliv že si bude současně data ukládat i jiná webová stránka B nebo C. Nelze totiž předem určit, jaké webové stránky budou své cookies třetích stran ukládat, přičemž se může jednat i o webové stránky, na které uživatel nikdy nevstoupil a ani vstoupit v budoucnu nemusí. V důsledku cookies třetích stran však o něm budou i tyto webové stránky zpracovávat data.

Tento problém je o to větší, že množství stran, které cookies třetích stran do zařízení uloží, může být v řádu desítek nebo i stovek. Uživatel, který tak bez rozmyslu odklikne vyskakovací okno s žádostí o souhlas, nevědomky otevřel stavidla pro sledování nejen konkrétní webové stránce, na kterou přistoupil, ale i velkému množství dalších subjektů. Problém je navíc násoben tím, že každá z těchto webových stránek potenciálně může data sdílet se svými „partnery“ napříč internetem. Není proto divu, že se ve společnosti postupně rozšířilo povědomí o negativním vlivu cookies třetích stran. Jednotlivé prohlížeče proto postupně na tuto poptávku veřejnosti reagovaly a ve svém výchozím nastavení začaly cookies třetích stran zakazovat. Druhý i třetí nejrozšířenější prohlížeč na trhu, tedy prohlížeče Safari a Firefox, zablokovaly ve svých nastaveních cookies třetích stran již v roce 2013.⁵ Tímto vstřícným krokem směrem k soukromí svých uživatelů tak *de facto* z pozice definiční autority zamezily v pokračování těchto nepřiměřených zásahů do soukromí uživatelů.⁶

1. Vzestup FLoC

Není náhodou, že poslední prohlížeč, který se k zákazu cookies třetích stran odhodlal, byl začátkem roku 2020 Google Chrome (dále jen „Chrome“). Ten v rámci iniciativy Privacy Sandbox (usilující o omezení sledování uživatelů napříč weby) tehdy deklaroval, že do dvou let také zakáže cookies třetích stran.⁷ Chrome, který však již tou dobou byl domi-

⁴ CARDLYTICS. Third-Party Cookies and Their Impact on Privacy. In: *Cardlytics* [online]. 25. 3. 2022 [cit. 2022-12-04]. Dostupné z: <<https://www.cardlytics.com/blog/third-party-cookies-and-their-impact-on-privacy/>>; NOUWENS, Midas et al. *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*. CHI 2020 Paper, Honolulu, April 25–30, 2020, s. 5. Dostupné z: <<https://people.csail.mit.edu/ilaria/papers/Midas-MITCHI2020.pdf>>. DOI: 10.1145/3313831.3376321.

⁵ BUMP, Pamela. The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2022 Phase-Out. In: *blog.hubspot.com* [online]. 27. 7. 2022 [cit. 2022-12-06]. Dostupné z: <<https://blog.hubspot.com/marketing/third-party-cookie-phase-out>>.

⁶ POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, s. 12.

⁷ GOOGLE, INC. Building a More Private Web: A Path towards Making Third Party Cookies Obsolete In: *Blog Chromium* [online]. 2020, s. 1 [cit. 29. 3. 2020]. Dostupné z: <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>.

nantním prohlížečem, ovládajícím zhruba 60 % trhu,⁸ potřeboval přijít s jiným řešením, díky němuž by mohl dále prodávat online reklamu, která produkuje přes 80 %⁹ veškerých příjmů společnosti Google Inc. (dále jen „Google“).

Z toho důvodu byl představen projekt *Federated Learning of Cohorts* (dále jen „FLoC“), který měl nahradit cookies třetích stran tak, aby mohl Google i nadále poskytovat svým inzerentům behaviorální reklamu. Systém měl fungovat tak, že webové stránky nejprve pomocí cookies a dalších nástrojů prvních stran uživatele identifikují a přiřadí jim ID,¹⁰ které následně zařadí do skupin s ID dalších prohlížečů, jejichž uživatelé projeví obdobné zájmy. Těmto skupinám Google přezdívá „kohorty“ a je to základní stavební prvek jeho nového systému FLoC. Jakmile jsou totiž uživatelé zařazeni do kohorty, Google dále pracuje pouze s kohortou jako s celkem, a nikoliv s jednotlivými ID. Ani sám Google tedy není schopen v rámci kohorty identifikovat konkrétního uživatele, a tedy dále již necílí na jednoho uživatele, ale na kohortu uživatelů se stejnými zájmy. Každý uživatel je zařazen do většího množství kohort v závislosti na jeho zjištěných zájmech, které se budou postupně aktualizovat. Takovými kohortami může být například kohorta milovníků fotbalu, kohorta levicových ekonomů nebo kohorta zájemců o pilates. ID kohort se navíc mělo měnit každý týden na základě posledních aktivit uživatele a aktualizovat tak zařazení do jednotlivých kohort.¹¹ Výhodou tohoto systému je, že data uživatelů neměla být ukládána na externích serverech, ale ke generování ID prostřednictvím algoritmu SimHash mělo docházet pouze lokálně na koncovém zařízení uživatele. Údaje o kohortách, do kterých bude uživatel na základě jeho předešlého chování zařazen, sice mají být každému běžně dostupné v koncovém zařízení, ale Google Chrome nebude kohortám přidělovat žádné označení pojící se s materiálním důvodem pro jejich vznik. Kohorty dostupné v koncovém zařízení tak budou mít pouze formální označení jako např. A123, C228, nebo C340.

Google, který byl již v roce 2020 pod tlakem, aby cookies třetích stran ve svém prohlížeči také zakázal, se snažil své řešení FLoC prezentovat jako pro-uživatelský krok v zájmu podpory ochrany soukromí. Leitmotiv počínání Googlu však byl od počátku relativně zřejmý. Bylo jím hledání systému, který by anonymizoval uživatele pouze do té míry, aby bylo možné plně využívat přesné behaviorální cílení a nadále prodávat personalizovanou online reklamu.

Tento cíl FLoC naplnil velmi dobře. Nejenže pozdržel úplné zrušení cookies třetích stran o několik let (cookies třetích stran nebyly v Chromu dosud zrušeny!), ale poskytl Googlu zdánlivý punc společnosti snažící se o zlepšení uživatelského soukromí za současného dosažení kvality cílené reklamy na úrovni 95% účinnosti¹² oproti tradičnímu sledování uživatelů prostřednictvím cookies třetích stran.¹³ Tah je pro Google přínosný také

⁸ STATCOUNTER. StatCounter Global Stats – Browser, OS, Search Engine Including Mobile Usage Share. In: *StatCounter Global Stats* [online]. 2022 [cit. 2020-03-29]. Dostupné z: <<https://gs.statcounter.com>>.

⁹ GLOBALDATA. Google's Revenue (2002–2021). *LinkedIn* [online]. 2022 [cit. 4. 12. 2022]. Dostupné z: <<https://www.linkedin.com/company/globaldatapl/>>.

¹⁰ Jedná se o jedinečný identifikátor tvořený zpravidla alfanumerickou řadou znaků.

¹¹ TECHNOGLITZ. Co je FLoC společnosti Google a jak jste sledováni online? In: *TechnoglitZ* [online]. [cit. 2022-12-06]. Dostupné z: <<https://technoglitZ.com/czechrepublic/co-je-floc-spolecnosti-google-a-jak-jste-sledovani-online>>.

¹² SCHIFF, Allison. The Industry Reacts To Google's Bold Claim That FLoCs Are 95% As Effective As Cookies. In: *AdExchanger* [online]. 26. 1. 2021 [cit. 2022-12-09]. Dostupné z: <<https://www.adexchanger.com/online-advertising/the-industry-reacts-to-googles-bold-claim-that-flocs-are-95-as-effective-as-cookies/>>.

¹³ JEŽEK, David. Novou sledovací techniku Google FLoC odmítají Vivaldi, Brave i DuckDuckGo. In: *Root.cz* [online]. 16. 4. 2021 [cit. 2022-12-09]. Dostupné z: <<https://www.root.cz/clanky/novou-sledovaci-techniku-google-floc-odmitaji-vivaldi-brave-i-duckduckgo/>>.

ve vztahu k regulaci ochrany osobních údajů, které se FLoC elegantně vyhne. Regulace ochrany osobních údajů totiž dopadá pouze na fyzické osoby, které jsou dle čl. 4 odst. 1 nařízení č. 2016/679 obecné nařízení o ochraně osobních údajů (dále jen „GDPR“) identifikované nebo identifikovatelné. Díky tomu, že kohorty mají být záměrně nastaveny tak, že sdružují skupinu osob, která díky zavedeným interním mechanismům systému nikdy nemá být tak malá, aby byla schopna identifikovat jednotlivce, nikdy by tak nemělo docházet ke zpracování osobních údajů. Velice významný je však také další efekt systému kohort, který nemusí být na první pohled zřejmý. Je jím pohled nekalé soutěže.

Analýza a způsob využívání kohort, dostupných v koncových zařízeních, zůstane ve FLoC na schopnostech reklamního průmyslu. Jakákoliv marketingová společnost si tak sice může sama nastavit způsob svého cílení, nicméně se významná část reklamních operací přesune do prohlížeče koncového zařízení, a tudíž mimo jejich dosah. Je proto zřejmé, že když bude jednotlivé kohorty nastavovat a spravovat právě Google, marketingový nástroj Googlu bude pravděpodobně nejefektivnější. Google si tímto krokem pod svoji faktickou kontrolu stahuje další významné činnosti a data a umocňuje tak svůj vliv. V jeho dominantním prohlížeči (a tedy již ve všech relevantních prohlížečích) bude nastaven zákaz ukládání cookies třetích stran, což zásadně omezí jiné metody identifikace. Jiní potenciální soutěžitelé na poli online marketingu tímto přijdou o velice efektivní cookies třetích stran bez adekvátní náhrady. Alternativu pak naleznou pravděpodobně jen v analyzování kohort, v nichž však vždy bude mít náskok právě Google.

Tento krok je proto nutné posuzovat v kontextu čl. 102 Smlouvy o fungování Evropské unie (dále jen „SFEU“), který stanoví, že: „S vnitřním trhem je neslučitelné, a proto zakázané, pokud to může ovlivnit obchod mezi členskými státy, aby jeden nebo více podniků zneužívaly dominantního postavení na vnitřním trhu nebo jeho podstatné části.“ Vzhledem k tomu, že Google má na daném trhu dominantní postavení, dojde prostřednictvím nového systému kohort k dalšímu omezení vlivu ostatních soutěžitelů, což dle mého názoru naplní výše uvedenou definici zneužití dominantního postavení.

2. Kritika a pád FLoC

Po představení systému FLoC si Google vysloužil řadu nesouhlasných reakcí a výzev k bojkotu nového systému.¹⁴ FLoC schytl kritiku například od významné mezinárodní neziskové organizace Electronic Frontier Foundation (EFF), která ve svém blogu uvedla, že v kohortách vidí pouze nový systém sledování, který nahradí starý systém sledování bez pozitivního vlivu na ochranu soukromí uživatelů.¹⁵ EFF pak konkrétně upozornil na možné kombinování metody fingerprintingu¹⁶ s již uloženými skupinami kohort v prohlížeči. Pomocí řady kohort, do kterých bude uživatel zařazen a které budou dostupné

¹⁴ COOKIEYES. Google FLoC: A Third-Party Cookie Alternative. In: *CookieYes* [online]. 17. 6. 2022 [cit. 2022-12-11]. Dostupné z: <<https://www.cookieyes.com/blog/what-is-google-floc/>>.

¹⁵ CYPHERS, Bennett. Google's FLoC Is a Terrible Idea. In: *Electronic Frontier Foundation* [online]. 3. 3. 2021 [cit. 2021-03-11]. Dostupné z: <<https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea>>.

¹⁶ Fingerprintingem se rozumí metoda identifikace koncového zařízení spočívající ve využívání technických údajů o zařízení, které jsou dostupné při přístupu zařízení na webovou stránku. Kombinací jednotlivých technických údajů, jako je například aktuální verze prohlížeče, MAC adresa, šifra zobrazované úhlopříčky a mnoho dalších údajů, lze uživatele s vysokou pravděpodobností identifikovat. Více viz KLODWIG, Jakub. *Ochrana soukromí v kontextu koncových zařízení uživatelů*, s. 30.

v koncovém zařízení, se totiž znatelně zvýší úspěšnost fingerprintingu, čímž bude uživatel touto metodou identifikován mnohem přesněji než dříve.

V článku s názvem *No, Google! Vivaldi users will not get FLoC'ed*. společnosti Vivaldi Technologies, provozující freewarový multiplatformní internetový prohlížeč, Vivaldi deklaruje, že FLoC nebude na prohlížeči Vivaldi funkční. Odůvodňuje to tím, že se FLoC spoléhá na některá skrytá nastavení v prohlížeči, která Vivaldi blokuje.¹⁷ Upozorňuje také na to, že Chrome musí volat servery Google, aby zkontroloval, zda může být spuštěn, jelikož Google FLoC zatím spustil pouze v těch částech světa, které nespádají do působnosti nařízení GDPR.¹⁸

Vivaldi pak shrnuje, že zatímco dosud se k profilování používaly cookies a local storage,¹⁹ FLoC toto pouze integruje do nitra prohlížeče Chrome, který profiluje uživatele na základě mnohem většího množství dat. Kohorty totiž budou agregovat data i z těch webů, které dříve cookies třetích stran nepoužívaly, a proto bude docházet k profilování prostřednictvím daleko většího množství webů, a tedy i na základě většího množství dat.²⁰

Další zajímavé vymezení se pochází od prohlížeče Brave, který slovy svého zakladatele a tvůrce JavaScriptu, Brendana Eich, hovoří o FLoC jako o promarněné šanci, nepochopení konceptu ochrany soukromí a škodlivosti pro koncové uživatele.²¹ Brave tak ve svém blogovém příspěvku otevírá problematiku zpracování zvláštních kategorií osobních údajů podle čl. 9 GDPR. Těmito údaji, které zahrnují například informace o zdravotním stavu, sexuální orientaci, politických názorech nebo o víře, se Google ve tvorbě svých kohort chce vyhnout tak, že kohorty s tímto citlivým obsahem nebude vytvářet, nebo upravovat algoritmus, který kohorty vytváří tím způsobem, aby takové korelace omezil.²²

Jak ale Brave trefně uvádí, rozhodnout, že jsou určité osobní údaje citlivé a nebude z nich generovat kohortu, může Google pouze po tom, co tyto údaje z koncového zařízení zpracuje a analyzuje. Navíc vytváření výčtu citlivých údajů je vysoce problematické a ve společnosti relativně subjektivní. Zatímco zařazení jedné osoby do kohorty sdružující lidi se zájmem v dívčím oblečení může zrcadlit jednoduše ženské pohlaví uživatelky, v jiném případě se může jednat o velice citlivou informaci o dospívajícím chlapci. Stejně tak zařazení v kohortě se zájmem o malé děti může sdružovat jak pediatry, tak i pedofily, a proto je zařazení určité informace mezi osobní údaje dle čl. 9 GDPR velice morálně ale i právně problematické. Brave proto pokládá otázku, kdo je Google, aby mohl rozhodovat, které informace o koncových uživateli jsou citlivé a které nejsou.²³ Kontext je proto důležitý a cílení na základě citlivých dat by mohlo snadno vést k diskriminaci.

Reklama nastavená na základě těchto citlivých dat by navíc mohla koncovým uživatelům velice přitížit. Pokud by se například zobrazovaly teenagerovi na jeho mobilu a počítači reklamy na ženské oblečení a mohli to zahlédnout jeho spolužáci, nebo pokud by Rusa

¹⁷ VON TETZCHNER, Jon. *No, Google! Vivaldi users will not get FloC'ed*. In: *Vivaldi Blog* [online]. 13. 4. 2021 [cit. 2022-12-10]. Dostupné z: <<https://vivaldi.com/blog/no-google-vivaldi-users-will-not-get-floced/>>.

¹⁸ COOKIEYES. *Google FLoC*.

¹⁹ Jako *local storage* je označováno úložiště ve webovém prohlížeči uživatele, ke kterému může být přístupováno pouze prostřednictvím uživatele.

²⁰ VON TETZCHNER, Jon. *No, Google! Vivaldi users will not get FloC'ed*.

²¹ EICH, Brendan – SNYDER, Peter. *Why Brave Disables FLoC*. In: *Brave Browser* [online]. 12. 4. 2021 [cit. 2022-12-10]. Dostupné z: <<https://brave.com/why-brave-disables-floc/>>.

²² MARCOSCACERES. *Excluding sensitive categories*. In: *Web Incubator CG* [online]. 2022 [cit. 2022-12-10]. Dostupné z: <<https://github.com/WICG/floc>>.

²³ EICH, Brendan – SNYDER, Peter. *Why Brave Disables FLoC*.

přístupujícího k určitým webovým stránkám, které dříve cookies neshbíraly, začal FLoC řadit do kohorty podporující NATO. Plošnost sběru dat FLoC, jejich přístupnost v prohlížeči a efekt na zobrazovaný obsah tak nemusí ve výsledku narušovat pouze soukromí, ale může mít i další zásadní dopady.

Z výše uvedených důvodů byl projekt FLoC velice kritizován již od svého představení. Žádný z velkých prohlížečů včetně Opery, Mozilly Firefox či Applu nevyjádřil podporu projektu FLoC, přičemž naopak Brave, Vivaldi, DuckDuckGo a Microsoft Edge jej ve svých prohlížečích zakázaly. Další významné technologické společnosti jako Oracle nebo WordPress jej aktivně kritizovaly, či dokonce chystaly jeho blokaci.²⁴

Poslední ranou pro FLoC pak pravděpodobně bylo vyšetřování Evropské komise. Ta se snažila zjistit, zda Google neporušil pravidla hospodářské soutěže EU tím, že si uživatelská data na webových stránkách a v aplikacích vyhradil pro vlastní zpracování pro reklamní účely a omezil k nim tak přístup třetích stran.²⁵ Google totiž shromažďuje údaje pro účely cílené reklamy, prodává reklamní prostor a působí také jako zprostředkovatel online reklamy, a je tedy přítomen na všech úrovních dodavatelského řetězce online grafické reklamy.²⁶ Tím může být ohrožen čl. 102 SFEU zakazující zneužívání dominantního postavení. Vyšetřování Evropskou komisí bylo zahájeno již 22. 6. 2021, ale vzhledem k tomu, že právo nestanoví žádnou lhůtu pro možné trvání antimonopolního šetření, není jisté, kdy bude zveřejněn jeho výsledek.²⁷ Vyšetřování Evropskou komisí spolu s řadou dalších žalob stran soukromých marketingových společností každopádně nakonec vedlo k rozhodnutí Google FLoC zrušit a začít vyvíjet nové odlišné a pravděpodobně i dobrovolné řešení, nazývané Google Topics.²⁸

Závěr

Po představení projektu FLoC, kterým Google zamýšlel nahradit cookies třetích stran, se zvedl silný odpor ze strany odborné veřejnosti i soukromých společností, který způsobil, že Google zvládl projekt FLoC spustit jen v testovací verzi, se zpožděním a pouze v některých státech, kde není platné nařízení GDPR. Po dalších problémech, kritice, žalobách a vyšetřování ze strany Evropské komise Google nakonec v lednu 2022 definitivně oznámil, že s projektem FLoC končí.

Toto oznámení ale nemůže být bez dalšího, jelikož se již dříve Google zavázal cookies třetích stran ve svém prohlížeči Chrome zakázat, což ale nemůže udělat, aniž by před-

²⁴ COOKIEYES. *Google FLoC*.

²⁵ EUROPEAN COMMISSION. Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct by Google in the Online Advertising Technology Sector. In: *European Commission* [online]. 22. 6. 2021 [cit. 2022-12-09]. Dostupné z: <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143>.

²⁶ KAYE, Kate. Why Google's Approach to Replacing the Cookie is Drawing Antitrust Scrutiny. In: *Digiday* [online]. 2. 2. 2021 [cit. 2023-01-28]. Dostupné z: <<https://digiday.com/media/why-googles-approach-to-replacing-the-cookie-is-drawing-antitrust-scrutiny/>>.

²⁷ Naposledy 14. 6. 2023 zveřejnila Evropská komise tiskovou zprávu uvádějící, že Google na poli online reklamy porušuje v Evropské unii regulaci hospodářské soutěže, a nastínila možné řešení v povinném prodeji části služeb Google. Viz EUROPEAN COMMISSION. Antitrust: Commission Sends Statement of Objections to Google over Abusive Practices in Online Advertising Technology. In: *European Commission* [online]. 2023 [cit. 2023-06-14]. Dostupné z: <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207>.

²⁸ TOWNSHEND, Pete. Google Topics API: Everything you need to know. In: *SmartFrame* [online]. 8. 2. 2022 [cit. 2022-12-04]. Dostupné z: <<https://smartframe.io/blog/google-topics-api-everything-you-need-to-know/>>.

stavil jiný alternativní systém, který by dále živil jeho miliardový business, postavený na online reklamě. Google se proto nyní upíná k cílené inzerci, založené na zájmech koncových uživatelů. Nový systém, který by měl být přívětivější k soukromí koncových uživatelů, se nazývá Topics a měl by být podle předběžných prohlášení na rozdíl od FLoC dobrovolný.²⁹

Pokud tedy projekt FLoC něco přinesl, pak je to poznání, jak důležitá je aktivita odborné veřejnosti a její dohled nad novými projekty, zejména v oblasti informačních technologií. Bude proto důležité sledovat vývoj metod identifikace koncových zařízení, diskutovat a i nadále se zasazovat o ochranu soukromí.

²⁹ Ibidem.

Replacing Third-party Cookies with Google's Ambitious FLoC System

Jakub Klodwig (<https://orcid.org/0000-0002-9599-2043>)

Abstract: Identification of end user devices online and targeting their users is a significantly evolving area that affects the daily lives of billions of people. Under public pressure, technology companies are banning the use of privacy intrusive third-party cookies and coming up with new methods and entire systems for online targeting and behavioural advertising. However, new does not necessarily mean better, it can bring additional or permanent privacy restrictions, as Google has attempted to do with FLoC (Federated Learning of Cohorts). This article explains the workings of FLoC, which Google planned to use to address the push to ban third-party cookies in its dominant browser, Google Chrome. The sophisticated system of cohorts that Google had been working on for years was intended to completely replace third-party cookies while further improving Google's position in the online marketing market. Not only would Google's implementation of the cohort system worsen the position of other companies offering online behavioural advertising, as they would have to rely on the data provided by the Google Cohort system, but at the same time the new system completely avoided data protection regulation. What changes, cracks, and risks the cohort system was supposed to bring, how members of the professional community as well as other competitors reacted, and what ultimately caused Google to reject its new cohort system, this article attempts to map and discuss from a privacy perspective.

Keywords: privacy, Google, cookies, online marketing, ePrivacy, cohorts, Google Topics