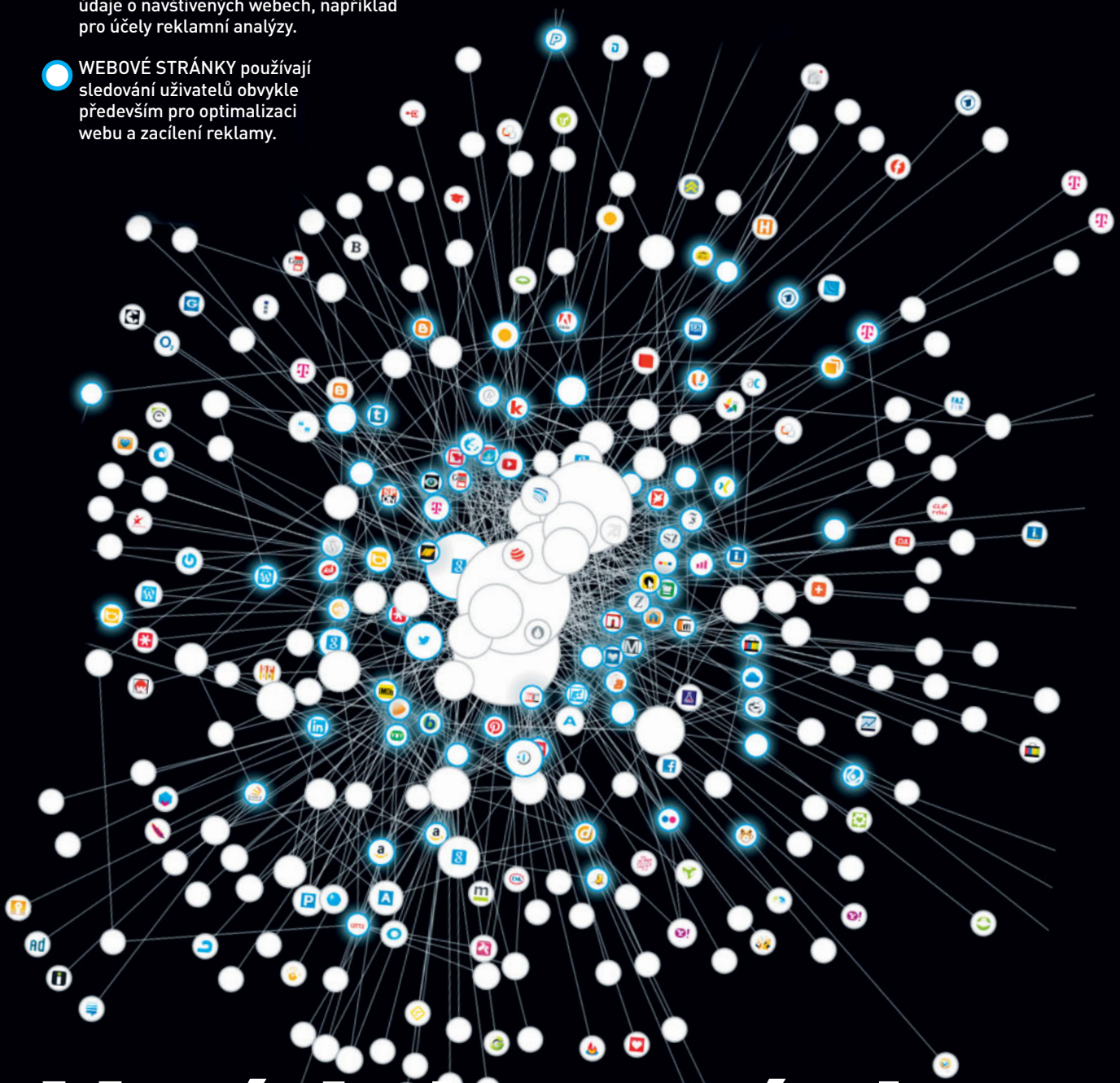
TRACKER
speciální služba, která zaznamenává údaje o navštívených webech, například pro účely reklamní analýzy.

WEBOVÉ STRÁNKY používají sledování uživatelů obvykle především pro optimalizaci webu a zacílení reklamy.



V síti datových DEALERŮ

TOP 50 DATOVÝCH ČMUCHALŮ

Naše analýza nabízí informaci, kolik webových trackerů lze najít na 100 webových stránkách. Seznam ukazuje, kolik trackerů vás přímo či nepřímo sleduje na vašich toulkách internetem.

Pořadí	Tracker	Sledovaných webů	Zodpovědná firma
1	googleanalytics.com	87	Google
2	qservz.com	74	Quisma
3	scorecardresearch.com	73	TMRG
4	atdmt.com	73	Microsoft
5	adition.com	70	Virtual Minds AG
6	googleadservices.com	70	Google
7	ytimg.com	70	Google
8	adrolays.de	70	abilicom
9	freenet.de	70	Freenet
10	feedburner.com	70	Google
11	googlesyndication.com	69	Google
12	gstatic.com	69	Google
13	adscale.de	69	Adscale
14	adnxs.com	69	AppNexus
15	amgdgt.com	69	Adconion Media
16	bp.blogspot.com	69	Google
17	blogblog.com	69	Google
18	serving-sys.com	69	MediaMind
19	ebaystatic.com	69	eBay
20	c-and-a.com	69	Cofra Holding
21	adsrvr.org	69	GoDaddy
22	advolution.biz	69	Media Ventures
23	invitemedia.com	69	Google
24	yimg.com	69	Yahoo
25	metalyzer.com	69	Metapeople
26	adrdgt.com	69	GoDaddy
27	adjug.com	69	AdJug
28	2mdn.net	68	Google
29	doubleclick.net	68	Google
30	yieldmanager.com	68	Yahoo
31	mythings.com	68	MyThings
32	google.de	68	Google
33	googleusercontent.com	68	Google
34	blogger.com	68	Google
35	youtube.com	68	Google
36	ivwbox.de	44	IVW
37	fbcdn.net	28	Facebook
38	akamaihd.net	28	Akamai
39	facebook.com	27	Facebook
40	nuggad.net	24	Nugg.ad
41	revsci.net	19	AudienceScience
42	admeld.com	19	Google
43	rubiconproject.com	19	Rubicon Project
44	openx.net	18	OpenX
45	amazon-adsystem.com	17	Amazon
46	pubmatic.com	17	PubMatic
47	ajax.googleapi.com	16	Google
48	webtrekk.net	15	Webtrekk
49	wunderloop.net	14	AudienceScience
50	quality-channel.de	13	Spiegel Verlag

* ZDROJ: ALEXA.COM

V obchodě s on-line reklamou, ve kterém se točí miliardy eur, jste analyzováni při každém kliknutí – tedy pokud se tomu nebráníte.

CLAUDIO MÜLLER

Výprava za nákupy do města bývá často otravná a pro většinu běžných nakupujících jde o nápor na nervy: narvané obchody, ukňourané děti a ve finále zboží, které se vám líbí, ale zrovna je nemají ve vaší velikosti. Přesto má klasické nakupování jednu výhodu: nejste při něm neustále sledováni maskovanými špiony, kteří si na každém vašem kroku poznamenávají podrobné informace o zboží, které jste si vyzkoušeli nebo na které jste se podívali. Pro většinu lidí je takováto představa děsivá, bohužel ale právě to se děje při nakupování na internetu. Špiony jsou firmy, které zobrazují reklamy na webových stránkách a analyzují chování uživatelů. Jednu z hlavních rolí v této oblasti hraje například Google.

Nástroji špionů jsou cookies, detekce prohlížeče a identifikace mobilního telefonu, výsledkem jejich práce pak konkrétní cílené reklamy na výrobky, o které jste se předtím zajímali, zobrazované na různých stránkách. Často jde přitom o takový nátlak, až máte chuť důrazně reklamě vysvětlit, že ty kalhoty jste si už dávno koupili a že by vás už konečně měla přestat pronásledovat.

Obecně lze on-line obchody považovat za oblast, která ze sledování těží nejvíce (a také ho nejvíce využívá). Sledování například odhalí, jak se uživatel na stránku obchodu dostal: zda prostřednictvím blogu, reklamního poutače na jiném webu, nebo přes vyhledávání na Googlu. Samozřejmostí je informace, co uživatel v obchodu dělal: díval se jen na jeden výrobek, nebo porovnával několik produktů mezi sebou? Hledal nějakou konkrétní značku? Kolik času strávil ve kterém oddělení?

Odborníci na reklamní marketing tato data analyzují a poté už uživatele bombardují produkty a speciálními nabídkami tohoto obchodu na jiných webových stránkách. Každý reklamní banner je poté malým útokem na vaši odolnost vůči lákavé nabídce.

„Předpokládá se, že jen asi dvě procenta všech návštěvníků obchodů koupí něco okamžitě," říká Norman Noetzold, zakladatel a šéf vývoje marketingové agentury Quisma (2. pořadí v žebříčku Top 50 vlevo). Podle Noetzolda se pomocí této metody lákání zákazníka (označované jako retargeting) může frekvence nákupu zvýšit o více než 10 procent. Uživatelé se podle jeho slov naštvou až tak po pátém opakování reklamy.

Sledovaný uživatel

Pro nezasvěceného je on-line reklama téměř tajnou vědou. Je tomu tak například i proto, že kromě zmiňovaného retargetingu existují i další, speciální typy reklamy. Třeba kontextová reklama se vztahuje k obsahu právě zobrazené stránky, tzv. keyword-targeting zase funguje na základě zadání a zvýraznění jednotlivých slov, stejně jako je tomu ve vyhledávači Googlu nebo Gmailu. A konečně je zde i tzv. behavioral targeting, tedy behaviorální cílení, při kterém se stopaři pokoušejí určit zájmy uživatele podle vzorce jeho chování. Pochopením tohoto vzoru chování se zabývají odborníci, jejichž profese se jmenuje customer journey manager. Mohli bychom je také nazývat tajnými společníky na ces-

tách po internetu, protože provádějí surfaře po stránkách internetu podobně jako průvodce provádí neznalé turisty orientálním bazarem. On-line reklamy, které jsou hlavním zdrojem příjmů mnoha webových stránek, jsou dnes většinou placeny podle počtu kliknutí nebo podle nákupů, na které nalákaly uživatele. Tyto reklamy tvoří v současné době přibližně dvě třetiny celosvětového inzertního obratu. Zjednodušeně lze říci, že čím více kliknutí, tím více peněz pro webovou stránku. A že nejde jen o pár drobných, o tom svědčí například i bilance Googlu, který v první polovině roku 2012 sám celosvětově na této reklamě vydělal 20,8 miliardy dolarů. Většina uživatelů se shodne na tom, že personalizovaná reklama nemusí být sama o sobě špatná – pokud je opravdu relevantní, může vám umožnit levně nakoupit zboží podle vašich představ.

Největším problémem je ale to, že uživatel sám nemůže dát svolení ke sběru informací o sobě, a nikdo se ho ani neptá, zda reklamu chce skutečně vidět. Vše je pouze v rukou obchodníků a reklamních agentur.

Profil uživatele vytvořený z drobků dat

Základem každé analýzy uživatele pomocí navštívených webových stránek jsou cookies (viz přehled vpravo). Když navštívíte webovou stránku, server této stránky uloží do vašeho počítače cookies, případně si přečte informace v již uloženém souboru cookie.

Stejnou věc dělají i reklamní stopaři, kteří při vstupu na stránku s reklamou na pozadí obvykle ukládají v cookies data o uživateli. Tyto cookies existují v celé řadě variant, počínaje nejjednodušími HTTP cookies. Jde o malé textové soubory, které často obsahují jen základní informaci, jako je datum nebo čas vstupu na stránku. Jiné cookies ukládají přihlašovací údaje nebo obsah nákupního košíku, aby konkrétního uživatele identifikovaly v různých sekcích webu.

Samozřejmě ale slouží i k jinému účelu. Pomocí cookies mohou být i anonymní uživatelé přeměněni na balíky dat, díky kterým mohou být jejich cesty analyzovány. Lze tak například zjistit, co nejčastěji návštěvníci hledají, co si obvykle prohlíží a na kterých stránkách tráví nejvíce času. Je také důležité zmínit, že cookies jsou obecně omezeny několika podmínkami – například každý web může číst pouze data ze svých cookies, nikoliv z okolních. Cookies by také měly mít omezenou dobu platnosti – pravda ale je, že většina webů se ji snaží nastavit co nejdelší. Lze bez problémů najít stránky, které mají u cookies nastavenu dobu úschovy až dvacet let! To ale zdaleka není nejnebezpečnější metoda sledování.

Stále oblíbenější metodou sledování uživatelů je využívání tzv. Flash cookies. Ty byly původně určeny především pro snadnější práci s webovými videi nebo pro ukládání informací souvisejících s internetovou zábavou (Flash hry). V současnosti jsou ale využívány především pro sledování uživatele, protože ve srovnání s klasickými HTTP cookies mají celou řadu výhod: nikdy nevyprší jejich platnost, jsou nezávislé na prohlížeči, lze do nich uložit až 100 kB dat (HTTP cookies mají 4 kB) a nesmažou se při běžném mazání cookies v prohlížeči.

V současné době ale už celá řada webů používá ještě vlezlejší techniku sledování uživatele – tzv. supercookie. Tu lze přirovnat k noční můře uživatele, protože jde o sledování, kterému se téměř nelze bránit. Jde totiž o kombinaci několika technik (cookies, Flash, HTML5), které společně vytváří téměř nezničitelné úložiště informací. Pokud totiž část z nich smažete, mohou být na základě ostatních dat obnoveny do původní podoby. Díky tomu vás mohou na webu sledovat téměř vždy a všude. Největší vinu na tom má především HTML5, které nabízí obrovský úložný prostor (původně pro interaktivní webové aplikace), kam si aplikace mohou téměř bez jakékohokoliv omezení ukládat svá data.

Jak nepředstavitelný může být rozsah nasbíraných dat, jež už jsou v databázích firem, to dokazuje sledovací analýza, kterou provedl v sousedním Německu Fraunhoferův institut pro bezpečné informační technologie (SIT): nejagresivnější webový slídil je aktivní na 265 z 500 největších webových stránek. „Pokud je stejná cookie nainstalována na stránkách různých poskytovatelů služeb, agentura dokáže bez problémů rozpoznat konkrétního uživatele a špehovat jeho chování při surfování," říká Markus Schneider, zástupce vedoucího institutu SIT. Kde je zrada? Shromážděné údaje nezůstávají v rukách sledovací služby, ale putují spletitými cestami k jiným poskytovatelům reklamních služeb. To také ukazuje naše sledovací analýza pomocí doplňku prohlížeče Collusion (viz strana 35). Podle zákona sice nelze osobní údaje předávat bez souhlasu uživatele, to ale neplatí pro anonymní údaje (jakým je například kliknutí). Proto se obchodování s daty tolik daří.

Záplava cookies by mohla za nějakou dobu polevit, protože podle směrnice EU týkající se e-soukromí (soukromí v elektronickém světě) by reklamní soubory cookies měly být uloženy pouze se svolením uživatele. Celá řada zemí samozřejmě odmítá tuto směrnici začlenit do svého interního práva. Ačkoli směrnice EU vyžaduje od společností získání souhlasu uživatelů, v praxi musí uživatelé spíše aktivně u firem protestovat. My vám doporučujeme jednodušší způsob: pomocí několika triků datové slídiče eliminujte (viz strana 38). Je ale zřejmé, že tyto triky znají i marketingové společnosti a snaží se přecházet na nové metody sledování.

Téměř forenzní metodou je „otisk prstu" browseru. Sledovací služby dokážou vytvořit individuální otisk prstu prohlížeče pomocí celé řady údajů, které jsou přenášeny v průběhu načítání webových stránek. Údaje zahrnují IP adresu, číslo verze operačního systému, nainstalované verze rozšíření Flash, Javy a dalších doplňků prohlížeče, stejně tak i rozlišení obrazovky a nainstalované fonty. Tyto parametry umožňují obrovské množství kombinací, tudíž jen zřídka může nastat situace, že dva prohlížeče vypadají stejně.

Sledování uživatele přes satelit

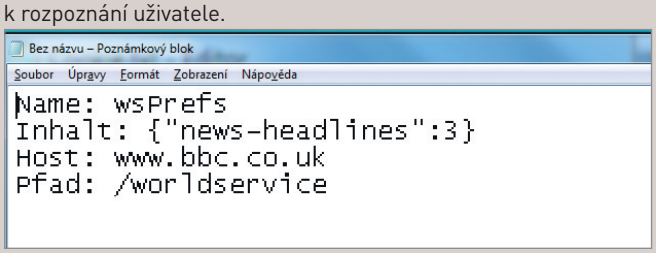
Prohlížeč, to je však jen začátek. Dalším cílem reklamních společností jsou mobilní zařízení. Obrovské množství uživatelů totiž surfuje na internetu prostřednictvím svých smartphonů. Výhodou smartphonu (z hlediska marketingových společností) je skutečnost, že tyto telefony většinou mají pouze jednoho uživatele a umožňují zcela novou analýzu jejich majitele přes Wi-Fi a GPS lokalizaci. Vzhledem k tomu, že na mobilních zařízeních mohou být soubory cookies uloženy pouze omezeným způsobem, cílená mobilní reklama se zatím zaměřuje pouze na aplikace, protože jen ty mohou exportovat velké množství dat. Bezpečnostní společnost BitDefender v listopadu analyzovala několik aplikací pro platformu Android, včetně populární hry Paradise Island, a zjistila celou řadu zajímavých skutečností. Například zmiňovaná hra zasílá telefonní čísla a e-mailové adresy na AirPush.com a identifikační číslo zařízení na Aark.net – což jsou poskytovatelé reklamních služeb specializující se na mobilní zařízení. Podle BitDefenderu není výjimkou, že aplikace exportují seznam kontaktů, stejně tak i navštívené

JAK SE VYTVÁŘÍ UŽIVATELSKÉ PROFILY

Pokud uživatel navštíví webovou stránku, datové trackery začnou analyzovat jeho chování na webu, konfiguraci jeho prohlížeče a počítače, aby mohly vytvořit specifický profil.

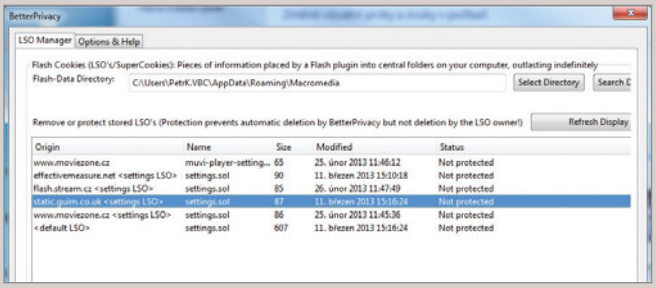
PŘEHLED COOKIES

Cookies jsou preferovaný typ nástroje na analýzu chování uživatele na webu. Webové stránky a sledovací služby je při nahrání stránky uloží na disk počítače a při příští návštěvě je použijí k rozpoznání uživatele.



HTTP COOKIE

ÚČEL	Identifikuje počítač přístupující ke stránce Řídí přihlašovací údaje (session cookie) Ukládá data pro substránky, jako například virtuální nákupní košíky
SKLADOVÁNÍ	Formát: textový soubor (txt) nebo SQLite databáze Místo: lokálně v prohlížeči, většinou v podsložce »C:\Uživatel\Username\AppData\« Maximální velikost: 4 KB



FLASH COOKIE

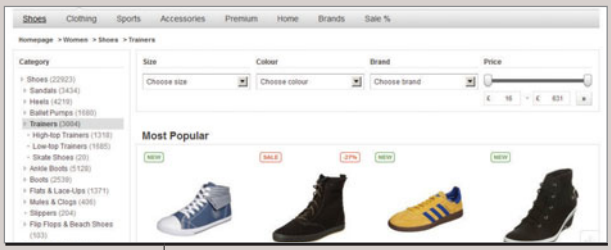
ÚČEL	Záznam pro Flash video a interaktivní hry Funguje nezávisle na prohlížeči Dokáže kopírovat a obnovovat HTTP cookies
SKLADOVÁNÍ	Formát: .sol Umístění: lokální složka přehrávače Flash player Maximální velikost: 100 KB

SUPERCOOKIE

ÚČEL	Identifikace uživatele a datový prostor pro webové aplikace
SKLADOVÁNÍ	Formát: SQLite databáze Umístění: přímo v prohlížeči (využívá HTML5 funkci DOM Storage) Maximální velikost: 10 MB

KDO VÁS SLEDUJE PŘI NAKUPOVÁNÍ?

Abychom zjistili, jak jsou na tom z hlediska sledování nakupující, vybrali jsme si typický zahraniční internetový obchod – nakupovací portál Zalando. V tabulce dole si můžete prohlédnout, kdo vás při nakupování pozoruje.



360YIELD	nizozemský obchodník
ADSCALE	německý obchodník
APPNEXUS	americký obchodník
ATDMT	tracker webové služby Microsoftu Atlas
ATEMDA	švédský obchodník
CRITEO	francouzský obchodník
DEMDEX	sledovač od Adobe
DOUBLECLICK	reklamní služba Googlu
FACEBOOK	sledování přes tlačítko „to se mi líbí“
METRIGO	německý obchodník
OPENX	americký obchodník
PUBMATIC	sledovač amerického webového hostingu GoDaddy
SMART ADSERVER	mezinárodní obchodník
SOCIOMANTIC	německý obchodník
YIELDLAB	německý obchodník
YIELDMANAGER	obchodník Yahoo

Pokud například hledáte zahraniční dopravní spojení, je běžné že v reklamním okně dalšího webu uvidíte cílenou reklamu.

webové stránky a požadavky na vyhledávání. Několik agresivních adwarových aplikací jde ještě dále a mění standardní vyhledávač tak, aby marketingové firmy mohly sledovat každý vyhledávací požadavek uživatele.

Za nejcennější informaci se však považuje lokalizace uživatele. „Vytváření uživatelských profilů je velmi jednoduchou záležitostí, pokud se dá sledovat místo výskytu uživatele. Tak se totiž dá zjistit hodně o tom, co byste rádi dělali," říká Liviu Arsene, bezpečnostní výzkumník firmy BitDefender. Pokud datový tracker například lokalizuje smartphone třikrát na stadionu, pak je uživatel pravděpodobně fotbalový fanoušek. Více než o ženskou obuv se tedy bude zajímat o sportovní oblečení nebo vstupenky na stadion. Je tedy velká pravděpodobnost, že si na svém smartphonu reklamu prohlédne.

Google a zase Google

Stále více firem se pouští do analýzy uživatele prostřednictvím mobilních zařízení, včetně start-upu Adelphic. Tato firma analyzuje vzor chování uživatelů mobilních telefonů pomocí 30 signálů. Adelphic neodhaluje, které signály to jsou, pouze tvrdí, že dokáže pomocí algoritmu rozpoznat to, jak uživatel reagoval na předchozí reklamní nabídky. Tento nápad měl pro Google hodnotu 10 milionů amerických dolarů, protože tuto firmu v prosinci zakoupil. Technologie Adelphic může být u Googlu dalším krokem ke zpracovávání a vyhodnocování údajů, které společnost shromažďuje prostřednictvím svých mobilních služeb, jako jsou Google Latitude nebo Now.

Zajímavým trikem může být pro reklamní společnosti možnost kombinovat datové záznamy získané prostřednictvím aplikací a prohlížeče na různých zařízeních. Vzhledem k rostoucí fragmentaci využití zařízení (PC, notebook, tablet, smartphone) je pro reklamní společnosti stále obtížnější zasílat cílené, a tudíž lukrativní reklamy uživatelům.

Kamakshi Sivaramakrishnan, bývalý zaměstnanec Googlu, chce tohoto cíle dosáhnout prostřednictvím vlastního start-upu Drawbridge. Služba využívá statistické analýzy anonymních údajů, aby mohla sledovat uživatele přes několik zařízení. Za tímto účelem tedy analyzuje data cookies různých prohlížečů (PC, mobilní zařízení) a pomocí algoritmu kontroluje, zda dva soubory cookie mohou patřit k jedné a téže osobě. Pokud je pravděpodobnost vysoká, cookies se sloučí do jednoho datového záznamu. Ještě děsivější je ale to, že takovéto sledování uživatele může stále narůstat, protože podobný typ reklamy se brzy může dostat i na naše televizory.

Nejprve ale firmy potřebují něco vědět o divácích. Pravděpodobně i proto si Google (pro Google TV) a také Verizon, americký kabelový operátor, podaly žádost na patent, který popisuje, jak lze analyzovat diváky pomocí kamery a mikrofonů integrovaných v televizních zařízení nebo set-top boxech. Patent Verizonu uvádí dva příklady: partneři sledující televizi se začnou hádat, načež se jim zobrazí televizní komerční reklama na poradenství v partnerských vztazích. Druhá scéna: pár se spolu mazlí na gauči a v televizoru se vzápětí zobrazí reklama na antikoncepci.

V současnosti je spíše běžnou praxí než výjimkou, že firmy o sledování uživatelů mlčí, protože transparentnost prý ohrožuje jejich obchodní model. Fakt ale je, že pokud uživatel zaregistruje tracker a všimne si sledování, často se pak webu vyhýbá úplně. V praxi tak pravděpodobně existují dvě řešení: buď bude uživatel žít pod dohledem Velkého bratra, nebo sledování zablokuje pomocí vlastních zdrojů.

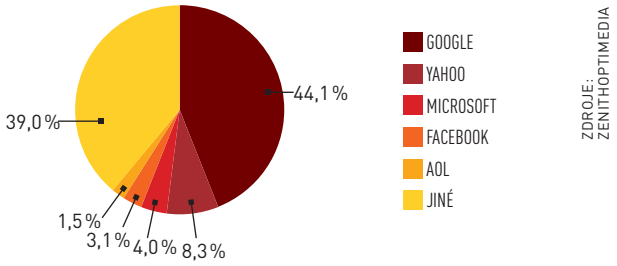
REKLAMNÍ SPOLEČNOSTI KOUPENÉ GOOGLEM

Google služby jsou obvykle zdarma, protože Google vydělává peníze prostřednictvím on-line reklamy. A to i proto, že převzal velké množství firem.

ROK	FIRMA	CENA	OBLAST PODNIKÁNÍ
2003	Applied Semantics	102 mil. USD	On-line reklama
2003	Sprinks	neznámá	On-line reklama
2006	dMarc Broadcasting	102 mil. USD	Reklama v rádiu
2007	Adscape	23 mil. USD	Reklama ve hrách
2007	DoubleClick	3,1 mld. USD	On-line reklama
2009	AdMob	750 mil. USD	Mobilní reklama
2009	Teracent	neznámá	On-line reklama
2010	Invite Media	81 mil. USD	On-line reklama
2011	Admeld	400 mil. USD	On-line reklama
2012	Wildfire Interactive	450 mil. USD	Reklama na soc. s.
2012	Adelphic	10 mil. USD	Cílení reklamy

PODÍLY NA TRHU Z HLEDISKA REKLAMNÍHO OBRATU

Žádná společnost nevydělá z reklamy na internetu tolik peněz jako Google. Facebook může o podobných číslech jen snít, a to navzdory tomu, že má miliardu uživatelů.



HROZBA BUDOUCNOSTI?

Velkým cílem reklamního průmyslu je v rámci analýzy spojit dohromady on-line a off-line aktivity uživatele – podobně jako u lokalizace smartphonu. Je však otázkou, zda metody popsané v patentu budou například v rámci Evropské unie legální či nikoliv. Pokud se to někomu může zdát neuvěřitelné, je nutné si uvědomit, že už existují firmy, které kombinují on-line uživatelská data (zjištěná z internetu) s těmi off-line, například z databází zásilkových firem a mobilních operátorů. Stačí si jen vzpomenout, kde jste podepisovali souhlas s poskytnutím svých údajů firmám třetích stran. Je tedy logické, že podle statistik společnosti KPMG se 90 procent uživatelů internetu obává o bezpečnost svých osobních údajů. I přes tuto nejistotu 56 procent spotřebitelů svěřuje s důvěrou své osobní údaje finančním institucím, třetina pak zabezpečeným platebním webovým stránkám (např. PayPal).

„Soukromí by nemělo být jen volitelné..."

GARY KOVACS, CEO Mozilla

PLACENÁ INZERCE

TIPY

Vyzrajte na sběratele dat

Pomocí jen několika klikutí budete mít kontrolu nad sledováním na webu, vymažete supercookies a zabezpečíte svůj mobilní telefon.

Je téměř nemožné zamezit veškerým únikům dat a sledování. Pomocí našich tipů si budete moci vytvořit takový profil, aby podle vašich požadavků zkombinoval uživatelskou přívětivost a zároveň přiměřenou ochranu soukromí.

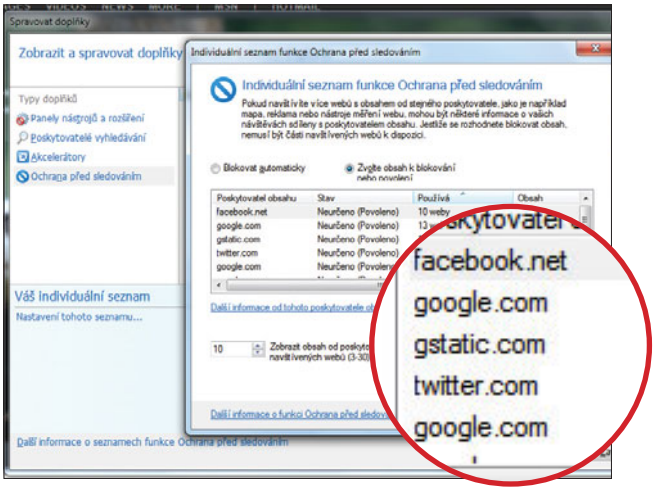
Odstraňte cookies (IE, Firefox, Chrome) – HTTP cookies můžete odstranit přímo v prohlížeči. V Internet Exploreru se jedná o nabídku »Nástroje | Odstranit historii procházení«, kde je nutné ve stejnojmenném okně přidat zatržítko u položky »Cookies« a kliknout na »Odstranit«. Firefox nabízí tuto možnost pod »Nástroje | Vymazat nedávnou historii«. V Chrome budete muset jít do nabídky »Přizpůsobení a ovládání Google Chrome | Historie | Vymazat všechny údaje o prohlížení | Smazat soubory cookie a jiná data webů a pluginů«. Odstranění Flash cookies takto jednoduché není, a proto budete ještě potřebovat doplněk typu BetterPrivacy (Firefox) nebo Click & Clean (Chrome). Tyto doplňky dokonce dokážou najít a odstranit supercookies pokaždé, když ukončíte prohlížeč.

Vypněte DOM Storage (Firefox) – možnost pro ukládání dat webových aplikací v prohlížeči (DOM storage) lze deaktivovat pouze ve Firefoxu. To provedete tak, že do adresního URL řádku zadáte »about: config«, v seznamu najdete parametr »dom. storage.enabled« a dvojitě na něj kliknete. To nastastaví hodnotu parametru na »False« a poté již webové stránky nemohou do počítače automaticky ukládat data.

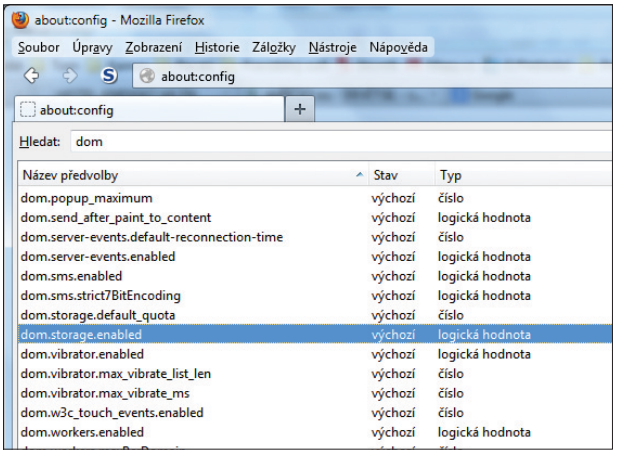
Aktivujte Ochranu před sledováním (Internet Explorer) – v tomto prohlížeči je nejlepší ochranou před trackery dat tzv. „Ochrana před sledováním“ z Fraunhoferova institutu. Tento doplněk najdete v nabídce »Nástroje | Spravovat doplňky«. Nástroj blokuje všechny uvedené trackery, jakmile se na internetových stránkách stanou aktivními. Seznam je automaticky aktualizován každé tři dny, takže v něm vždy najdete i ty nejnovější.

Konfigurujte mobilní zařízení (Android, iOS) – od konce listopadu již existuje šikovný blokátor reklam Adblock Plus (známý z internetových prohlížečů) i jako aplikace pro smartphony s operačním systémem Android. Aplikace blokuje reklamy na mobilních webových stránkách a dokonce i reklamní bannery v aplikacích. Kromě toho doporučujeme také deaktivovat lokalizační funkci GPS vašeho přístroje, pokud pro vás není nezbytně nutná. V iOS od verze 6 můžete rovněž omezit reklamní sledování. Příslušnou volbu najdete v nabídce »Nastavení | Obecné | Informace | Reklamy«.

AUTOR@CHIP.CZ



Tracking protection list v IE hledá a blokuje trackery na webových stránkách pomocí pravidelně aktualizovaných údajů.



V prohlížeči Firefox můžete ukládání dat (DOM storage) deaktivovat jediným kliknutím v »about: config«.

Ve smartphonech s OS Android byste měli vypnout GPS lokátor, abyste sledovacím službám zkomplikovali zkombinování těchto dat s uživatelským profilem.