Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

BAKALÁŘSKÁ PRÁCE

Jakub Skoček

Digitální stopy – možnosti kontroly a eliminace pomocí vybraných volně dostupných nástrojů

Digital footprints – Possibilities of control and elimination by selected freely available tools

Praha 2012

Vedoucí práce: PhDr. Pavla Kovářová

Chtěl bych velmi poděkovat PhDr. Pavle Kovářové, za to, že se mne ujala uprostřed rozdělané práce a po celou dobu jejího dokončování mi s velkou trpělivostí pomáhala cennými radami a připomínkami.

Prohlašuji, že jsem bakalářskou práci vypracoval/a samostatně, že jsem řádně citoval/a všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 2. 8. 2012 ……

podpis studenta

Abstrakt

Cílem bakalářské práce je zjistit, do jaké míry má uživatel možnost chránit své soukromí před negativními dopady spojenými se vznikem digitálních stop pomocí volně dostupných nástrojů. Na začátku je pojem digitální stopa zkoumán z několika úhlů pohledu, v závislosti na oborech, které ho využívají. Na základě těchto odlišností je pak stanovena definice termínu vhodná pro účely této práce. Následně je popsán vznik digitálních stop a rizika, která s sebou přinášejí. V další kapitole jsou nastíněny možnosti kontroly, zjištění rozsahu a případného odstranění digitálních stop uživatelem. V praktické části, která bezprostředně navazuje na předešlou kapitolu, jsou vybrány vhodné nástroje a vzájemným porovnáním je zjišťováno, zda je jejich prostřednictvím možné (případně do jaké míry) případným rizikům předejít a ochránit tak své soukromí.

Klíčová slova

Internet, osobní informace, soukromí, bezpečnost

Abstract

The goal of this bachelor thesis is to find out to what extent the user is able to protect his privacy against negative impacts linked to digital footprints, using tools that are available for free. At the beginning, the term digital footprint is investigated from several points of view, according to fields that use it. Based on these differences, the definition of the term is stated, suitable for the purpose of this work. Then the origin of the digital footprints, and connected risks, are described. In the next chapter, the opportunities of control, finding of scale, and possible remove of digital footprints by the user, are outlined. In the practical part, that immediately follows the previous chapter, the suitable tools are chosen, and by the mutual comparison, it is investigated whether it is possible (and if so, to what extent) to prevent possible risks and protect the privacy.

Keywords

Internet, personal informations, privacy, security

Obsah

1. Úvod

V rozmezí let 2000 až 2011 rapidně vzrostl celosvětový počet uživatelů internetu; konkrétně o 528.1 %[1]. Tento nárůst je důsledkem nejen stále větší dostupnosti internetového připojení a moderních technologií umožňujících využívat toto připojení prakticky kdekoliv, ale zejména změnou postavení samotných uživatelů ve vztahu k internetu jako médiu. S příchodem nové vývojové fáze, která bývá – navzdory neshodám v názorech odborné i laické veřejnosti – označována jako Web 2.0, se uživatel změnil z pouhého konzumenta na konzumenta - tvůrce, který obsah sám vytváří (či se na tvorbě alespoň podílí). Zatímco dříve byl obsah webových stránek tvořen především jeho správci a možnost interakce uživatele byla malá, nyní je situace opačná. Vlastnit dnes internetovou stránku, blog či profil na sociální síti je pouze otázkou elementárních znalostí práce s počítačem. Tento trend přesně vystihl zakladatel Socialtext Incorporated Ross Mayfield ve známé větě „Web 1.0 was commerce, Web 2.0 is people“[2].

Logickým důsledkem tohoto vývoje je velký nárůst množství volně dostupných informací, včetně informací osobních. Není tedy divu, že se tyto osobní informace staly v prostředí internetu vyhledávanou a velmi ceněnou komoditou a někteří odborníci je přirovnávají k „ropě internetu“[3]. Naše virtuální identita se tak rychle stává stejně důležitou, jako ta reálná (fyzická). Přesto si to mnozí uživatelé stále neuvědomují a považují internet za anonymní prostředí, kterým již dávno není.

K výběru tématu digitálních stop mě vedla nejen jeho aktuálnost, ale zejména fakt, že ačkoliv jsou tyto stopy vytvářeny při každém pohybu na internetu, mohou představovat zásadní riziko pro ochranu soukromí a jejich zneužití může mít fatální následky, mnoho lidí o nich nemá téměř žádné (či vůbec žádné) povědomí. V českém

---

1 World Internet Users and Population Stats. *World Internet Usage News and Population Stats* [online]. 2012, April 26, 2012 [cit. 2012-04-28]. Dostupné z: http://www.internetworldstats.com/stats.htm

2 SINGEL, Ryan. Are You Ready for Web 2.0?. *Wired* [online]. 10.06.2005 [cit. 2012-04-28]. ISSN 1059-1028. Dostupné z: http://www.wired.com/science/discoveries/news/2005/10/69114

3 *„Personal data is the new oil of the Internet and the new currency of the digital world.”* - Meglena Kuneva, European Consumer Commissioner.
WORLD ECONOMIC FORUM. *Personal Data: The Emergence of a New Asset Class*. 2011. Dostupné z: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

jazyce se zatím nevyskytuje žádný ucelenější materiál, zabývající se digitálními stopami, většina podkladů je pouze na úrovni článků v časopisech o informačních technologiích a neposkytují tak souhrnný náhled na tuto tématiku. Proto budu tuto práci koncipovat jako komplexní úvod do problematiky digitálních stop, který by bylo možné dále využít jako základ pro další výzkum či jako informační zdroj pro širší veřejnost. V teoretické části se budu zabývat vznikem digitálních stop, riziky jejich zneužití (zejména s přihlédnutím k fenoménu sociálních sítí), možnostmi kontroly a nástroji pro jejich eliminaci. V praktické části pak budu porovnáním vybraných volně dostupných nástrojů zjišťovat, do jaké míry má běžný uživatel možnost pomocí těchto nástrojů chránit své soukromí a osobní údaje před negativními dopady digitálních stop.

2. Digitální stopy a problematika definice podle oborů

Samotný pojem „digitální stopy“ není – snad s výjimkou forenzních věd – pevně definován. V nejširší rovině můžeme za digitální stopy považovat data (a metadata[4]), která vznikají při interakci uživatele s digitálním prostředím – počítačem, telefonem, ale i televizí[5]. Nicméně tato definice plně nereflektuje rozsáhlost tohoto pojmu, který je nyní dosti volně využíván v řadě oborů. V každé z těchto oblastí pak mají digitální stopy trochu jiný význam, který se odvíjí od úhlu pohledu dané disciplíny. Účelem práce není porovnávat jednotlivé definice, přesto je pro lepší pochopení okolností potřeba tyto rozdíly zmínit. Poté budu moci lépe a přesněji stanovit definici vhodnou pro tuto práci.

Pro demonstraci rozdílných pohledů jsem vybral tři obory, s nimiž je pojem digitální stopy často spojován: kriminalistika a forenzní vědy, marketing a počítačová věda. Zajisté můžeme nalézt více oborů, které pohlížejí na toto téma odlišně, nicméně, jak jsem již zmínil, porovnání není účelem práce a pro naši představu tyto tři postačí.

2.1. Kriminalistika a forenzní vědy

V kriminalistické a forenzní praxi jsou digitální stopy v první řadě brány jako důkazní materiál[6]. Nemusí se však nutně jednat o dokazování trestného činu; využití nacházejí také při řešení forenzního šetření, které provádí státní správa (například při občanskoprávních sporech), či pro potřeby nezávislých auditů v komerční sféře[7]. Zde však dochází ke sporu ve výkladu jednotlivých autorů i v rámci konkrétního oboru. Jedna strana považuje za digitální stopy pouze data, která jsou přímo spojena s trestným

---

4 Strukturovaná data o datech.

5 FISH, Tony. *My digital footprint*: *a two sided digital business model where your privacy will be someone else's business* [online]. London: Futuretext, 2009 [cit. 2012-04-28]. ISBN 978-095-5606-984. Dostupné z: http://31.222.183.71/footprint-cms/THE_BIG_PICTURE.html

6 Proto se také v zahraničí využívá označení „digital evidence“ (důkaz) místo „digital footprint“ (stopa). V českém prostředí se tyto výrazy příliš nerozlišují a i v odborných zdrojích jsou popisovány jako digitální stopy místo digitálních důkazů.

7 PORADA, Viktor a Roman RAK. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. *Karlovarská právní revue*. 2006, roč. 2, č. 4, 1 - 21. Dostupné z: http://mail.vskv.cz/download/KPR/archiv/2006/kpr4_2006.pdf

činem. Jak uvádí například Eoghan Casey[8]: „Za digitální důkazy považujeme jakákoliv digitální data, která mohou prokázat spáchání trestného činu nebo mohou poskytnout vazbu mezi trestným činem a jeho obětí či jeho pachatelem“. Druhou skupinu reprezentuje, dnes nejvíce využívaná a respektovaná definice pracovní skupiny *Scientific Working Group on Digital Evidence (SWGDE)*, podle které je digitální stopa: „Informace s vypovídací hodnotou, uložená či přenášená v digitální podobě“[9]. Do této definice pak můžeme zahrnout širokou škálu dat nejen z oblasti počítačové komunikace. Patří sem nejen samotné dokumenty, ale také „otisky“ činnosti, které zanechává prakticky každé technologické zařízení pracující s daty (např. souřadnice GPS, seznam hovorů, videozáznamy z bezpečnostních kamer), či metadata, která mohou obsahovat další důležité informace o daném souboru – např. u fotografie datum a čas pořízení, typ fotoaparátu a jeho nastavení.

2.2. Marketing

V marketingovém prostředí je pojem digitální stopy (ačkoliv zde není pevně definován) používán zejména v oblasti takzvaného behaviorálního[10] marketingu. Jedná se o typ marketingu, který je založen na sledování a následném analyzování chování uživatelů, využívaného pro zvýšení marketingové efektivity. Ze získaných informací jsou sestavovány profily, které reklamním společnostem umožňují doručovat personifikovaná reklamní sdělení. Samotná analýza probíhá většinou na základě dvou aspektů[11]: sledování klíčových slov zadávaných do vyhledávačů a sledování pohybu napříč navštívenými webovými stránkami (většinou se však vztahuje pouze na oblast spravovanou danou reklamní agenturou[12]). Oba typy sledování pak mohou poskytnout množství informací o zájmech uživatele. Digitální stopy zde tedy můžeme definovat jako data získaná sledováním aktivit uživatelů na internetu, která mají vypovídací

---

[8] CASEY, Eoghan. Computer Evidence and Computer Crime. In: PORADA, Viktor a Roman RAK. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. *Karlovarská právní revue*. 2006, roč. 2, č. 4, 1 - 21. Dostupné z: http://mail.vskv.cz/download/KPR/archiv/2006/kpr4_2006.pdf

[9] Vlastní překlad autora. FBI. Digital Evidence: Standards and Principles. *Forensic Science Communications* [online]. 2000, roč. 2, č. 2 [cit. 2012-04-28]. Dostupné z: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Definitions

[10] Z anglického slova „behaviour“ znamenajícího chování.

[11] Behaviorální marketing. In: *MediaGuru* [online]. 2012 [cit. 2012-04-28]. Dostupné z: http://www.mediaguru.cz/medialni-slovnik/behavioralni-marketing/

[12] Se sledováním a následným využitím získaných informací se můžeme setkat i na úrovni jednotlivých webů. Prvním příkladem mohou být elektronické obchody, které na základě již zobrazeného zboží umějí nabídnout zboží, které by mohlo zákazníka také zajímat.

hodnotu o uživatelských návycích a zájmech, ze kterých je následně možné sestavit jejich (více či méně přesný) profil, využitelný pro komerční účely.

2.3. Počítačová věda

Již svým přívlastkem digitální stopy jasně poukazují na vztah k počítačové vědě, počítačům a celé škále různých komunikačních zařízení, jejichž masový rozmach jsme mohli zaznamenat v poslední době. Společným znakem prakticky všech těchto moderních přístrojů je možnost přistupovat jejich prostřednictvím do sítě internet. A právě interakcí uživatelů v prostředí internetu (bez ohledu na použité zařízení) vznikají digitální stopy. Digitální stopu tvoří soubor informací, které za sebou uživatel zanechává (ať již vědomě, či nevědomě) během svého pohybu po síti[13]. Podle studie[14] amerického výzkumného centra Pew Research Center z roku 2007 můžeme rozdělit digitální stopy v online prostředí na dvě hlavní skupiny: ***aktivní*** a ***pasivní.***

> ***Aktivní digitální stopy*** jsou zde definovány jako: „Osobní údaje, zpřístupněné vědomým nahráváním a sdílením samotným uživatelem.“
>
> ***Pasivní digitální stopy*** jsou naopak definovány jako: “Osobní údaje zpřístupněné online, bez záměrného přičinění uživatele.“[15]

Jak z definic jasně vyplývá, autoři studie považují za digitální stopy výhradně osobní údaje, což je v tomto případě nedostačující. Ne všechna data a informace, které uživatelé sdílejí (a které samozřejmě také tvoří jejich stopu) mohou být považovány za údaje osobní[16]. Z tohoto dělení budu dále vycházet a poslouží mi jako základ pro vymezení pojmu digitální stopy vhodného pro tuto práci. Aby však bylo vymezení kompletní, je třeba jej doplnit i o jiné druhy informací.

Za aktivní stopy můžeme tedy považovat všechna data a informace, které souvisí s uživatelem a jsou jím samotným vytvořeny a zveřejněny. Zahrnují např. příspěvky

---

[13] ČERNÝ, Michal. Digitální stopy a digitální identita. *RVP*: *Metodický portál* [online]. 2011 [cit. 2012-04-28]. Dostupné z: http://clanky.rvp.cz/clanek/o/g/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html/

[14] MADDEN, Mary, Susannah FOX, Aaron SMITH a Jessica VITAK. *Digital Footprints: Online identity management and search in the age of transparency* [online]. Washington: Pew Internet & American Life Project, 2007 [cit. 2011-04-19]. Dostupné z WWW: http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Digital_Footprints.pdf

[15] Vlastní překlady autora.

[16] Jelikož nevedou k jednoznačnému určení osoby.

a komentáře na veřejných stránkách, blogy, osobní webové stránky, fotografie a videa nahraná a sdílená prostřednictvím patřičných serverů či členství v zájmových skupinách a fórech. Samostatnou skupinou jsou pak profily na sociálních sítích a podobných webových službách, umožňujících uživatelům vytvářet obsah, který je kombinací různého počtu výše zmíněných možností. Takový profil může sloužit jako osobní stránka či blog, a zároveň lze jeho prostřednictvím sdílet multimediální obsah, komunikovat s ostatními uživateli nebo se sdružovat ve skupinách.

Právě komunikace a sdílení obsahu mezi uživateli je hlavním funkcí sociálních sítí. Jejich prostřednictvím jsou zveřejňována i data, týkající se konkrétních uživatelů, která však nebyla nahrána jimi samotnými, ale dalšími osobami, obvykle z řad přátel. Podle výše zmíněné studie by pak tato data nespadala do skupiny aktivních digitálních stop, ale skupiny pasivních stop. Někteří autoři[17] však zahrnují data zveřejněná jinými osobami stále do skupiny aktivních stop (i když je tak přímo nenazývají). Důvodem bude zřejmě fakt, že se obvykle jedná o obdobné informace, jaké o sobě sdílejí sami uživatelé, jsou ve většině případů snáze vyhledatelné a uživatel nad nimi má jistou kontrolu, na rozdíl od mnoha stop pasivních. Jelikož se bude dělení na stopy aktivní a pasivní objevovat v průběhu celé práce, je třeba zmínit, že informace sdílené jinými uživateli budou dále považovány také za stopy aktivní.

Pasivní digitální stopy pak představují data, vznikající bez záměru (a často i bez vědomí) uživatele. Pomineme-li informace o uživateli sdílené další osobou, které ponechám zařazené ve skupině aktivních stop, jedná se zejména o záznamy aktivit uživatele v online prostředí - data představující výčet navštívených webových stránek, četnost a čas jejich návštěv, činnosti na jednotlivých stránkách (nastavení preferencí, vyplnění formulářů, jednotlivá kliknutí apod.) a související data jako IP adresa, poskytovatel připojení, lokace či kontext a provázání jednotlivých dat. V dnešní době může být jakákoliv aktivita v online prostředí zaznamenána a uložena. Pasivní stopy

[17] Tony Fish ve své knize Digital Footprint přímo vychází z dělení Pew Research Center.
FISH, ref. 5.
ČERNÝ, ref. 13.

pak mají, stejně jako aktivní, určitou vypovídací hodnotu o uživateli, který je zanechal. V tomto případě vypovídají o zájmech a návycích uživatele.

Pro účely této práce je digitálními stopami myšlen souhrn všech dat a informací zaznamenávajících uživatelovu interakci v online prostředí, které mohou být nějakým způsobem zachyceny a zneužity. Vzhledem k výrazným odlišnostem v procesu vzniku, možnostech kontroly ze strany uživatele, vyžadují odlišný přístup. V průběhu práce tak budou ve většině případů popisovány samostatně.

3. Rizika zneužití digitálních stop

Jedním z hlavních znaků dnešní společnosti je velmi otevřená (a často až nezodpovědná) komunikace informací mezi uživateli. Problémem tohoto přístupu je fakt, že v prostředí internetu prakticky nelze nic schovat, jednoduše proto, že to není *kam* schovat. V této kapitole nastíním důvody, proč je vůbec důležité znát své digitální stopy a proč by je měli uživatelé mít co nejvíce pod svou kontrolou.

Bezpečnostních rizik, která se nějakým (větším či menším) způsobem vážou k digitálním stopám, můžeme nalézt tolik, že není ani zdaleka možné zabývat se všemi v rámci bakalářské práce. Z tohoto důvodu jsem vybral tři zástupce vhodné k nastínění dané problematiky: sledování návyků uživatelů, využití osobních informací v personalistice, krádež identity. Tato rizika jsem zvolil záměrně, jelikož patří v literatuře k obvykle zmiňovaným možnostem zneužití digitálních stop v současnosti[19]; zároveň zahrnují oba druhy stop - aktivní i pasivní a dostatečně zobrazují rozmanitost možných dopadů na uživatele při zneužití stejného „prostředku“.

3.1. Sledování uživatelů

Sledování návyků uživatelů v online prostředí může být realizováno dvěma subjekty – navštívenou webovou stránkou (1st party) nebo takzvanými třetími stranami (3rd party), většinou reprezentovanými sběrateli dat a reklamními společnostmi. Webové stránky využívají tato data pro své potřeby, například pro statistické účely (návštěvnost, nejčtenější články atd.) a nemusí být předávány třetím stranám. Naopak pro třetí strany je získávání informací o zájmech uživatelů výnosným byznysem. Jeho rozvoj je důsledkem stále větší poptávky reklamních společností po tomto typu informací. Společnosti prodávající reklamu přecházejí, v neustálé snaze o zlepšení efektivity reklamního sdělení, od klasické kontextové reklamy[20] na reklamu cílenou, pro jejíž správné fungování jsou informace o uživatelských zájmech nezbytné. Z takto získaných informací jsou sestavovány profily, které mohou být rovnou využity pro

[19] ČERNÝ, ref. 17, 13.
Informační bezpečnost: Ochrana osobních údajů na internetu. *Elektra*: *Portál elektronických materiálů FF UK* [online]. 2011 [cit. 2012-07-30]. Dostupné z: http://elektra.ff.cuni.cz/ingram/informacni-bezpecnost/InfoBezpecnost.pdf

[20] Při kontextové reklamě je obsah reklamního sdělení vázán na obsah webu či služby, na které se zobrazuje; příkladem může být reklama na autobazar na motoristickém webu. Tento druh reklamy je tak alespoň částečně zaměřen na potencionální cílovou skupinu, čímž se zvyšuje jeho efektivita.

reklamní účely, nebo v případě subjektů (prezentovaných jak firmami, tak i jednotlivci) zabývajících se sběrem dat, k jejich dalšímu prodeji. Podle Julie Angwin, která se tématu sledování uživatelů v prostředí internetu dlouhodobě věnuje, vzniklo poslední dobou mnoho firem, zabývajících se nákupem, prodejem či výměnou takovýchto profilů. Každý den se na jednom takovém trhu (Blue Kai) prodá přes 50 miliónů informací o našich online návycích. Cena této informace se přitom pohybuje, v závislosti na obsahu, kolem jedné desetiny centu[21].

V roce 2010 zpracoval americký Wall Street Journal v čele s již zmíněnou Julií Angwin detailní studii[22], monitorující počet a původ jednotlivých sledovacích zařízení na padesáti nejnavštěvovanějších webových stránkách ve Spojených státech amerických[23]. Podle této studie je průměrný počet různých sledovacích zařízení na jedné stránce 64; dohromady jich pak všech padesát webů obsahovalo na 3,180. Více než dvě třetiny z nich (2,224) však pochází od třetích stran (konkrétně od 131 různých firem) a jen necelá třetina je instalována navštívenou webovou stránkou. Pouze jediný web ze všech testovacích, volně tvořená encyklopedie Wikipedia neobsahoval žádná sledovací zařízení. Na opačném konci skončil web Dictionary.com, který využívá 234 zařízení, z nichž 223 pochází od třetích stran

Ohrožení soukromí uživatele může nastat v případě, že je nashromážděno velké množství dat. V profilech jsou většinou ukládány informace typu geografické lokace, pohlaví, odhadovaného věku a zájmů; některé firmy však mohou doplňovat profily o své odhady týkající se příjmu, rodinného stavu či vlastnictví nemovitostí[24]. Tyto informace samy o sobě nejsou informace osobní[25], které by mohly vést k jednoznačné identifikaci konkrétní osoby. Nicméně při dostatečném množství informací, nebo při jejich kombinaci s jinými zdroji, se lze dobrat ke skutečné identitě takto sledovaného uživatele. Jak uvádí profesor Paul Ohm na příkladu profilu obsahujícího ZIP kód (můžeme přirovnat k českému poštovnímu směrovacímu číslu), pohlaví, věk a model

---

[21] ANGWIN, Julia. The Web's New Gold Mine: Your Secrets. *The Wall Street journal* [online]. July 30, 2010 [cit. 2012-01-04]. ISSN 00999660. Dostupné z: http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

[22] Výsledky průzkumu jsou v interaktivní formě dostupné na webové stránce http://blogs.wsj.com/wtk/

[23] Jelikož se ve většině případů jedná o stránky globálních společností, jako jsou Facebook, Microsoft, Yahoo!, Wikipedia a podobně, lze využít tyto výsledky i v našem prostředí.

[24] ANGWIN, ref. 21.

[25] Podle evropské legislativy, ze které vychází i český zákon č. 101/2000 Sb., o ochraně osobních údajů.

auta. Pokud použijeme ZIP kód, sníží se nám počet možných uživatelů na určité číslo, když přidáme pohlaví a věk, počet možných reálných osob opět klesne. Pokud přidáme ještě další informace, jako zmíněný typ auta, je tu jistá pravděpodobnost, že se dostaneme ke skutečné identitě[26].

I když firmy vymýšlejí stále sofistikovanější způsoby, jak skrytě zaznamenávat aktivitu uživatelů, nejpoužívanějšími nástroji pro tuto činnost jsou pořád soubory cookies a tzv. pixelový (internetový) tag[27].

3.1.1. Cookies

První soubory cookies vytvořil v roce 1994 Lou Montulli pro prohlížeč Navigator firmy Netscape, jejíž byl zaměstnancem. Do této doby byl jakýkoliv web bez „paměti" a opuštění stránky během relace znamenalo nemožnost na ní plynule navázat při další návštěvě. Web nemohl uživatele žádným způsobem identifikovat a jakékoliv přerušení znamenalo vykonat celou operaci od začátku. Lou Montulli vyřešil tento problém tak, že dal webovým stránkám možnost uložit malý textový soubor do uživatelského počítače. Tento soubor obsahuje unikátní číslo ID a další informace, které umožňují vzájemnou identifikaci mezi dvěma entitami – v tomto případě počítačem a konkrétním webem. Jiří Peterka[28] trefně přirovnává tento proces k návštěvě čistírny v reálném životě, kdy uživatel dostane určitý doklad, který při vyzvednutí předá personálu, jenž ho na jeho základě identifikuje a vydá příslušný oblek. V praxi nám tak dovolují například ukládat přihlašovací údaje, používat nákupní košík v e-shopech nebo personalizovat oblíbené stránky. Původní koncept cookies byl vytvářen s dobrým úmyslem zlepšit funkčnost webových stránek a zjednodušit tak uživatelům jejich práci s nimi.

Cookies můžeme rozdělit na dva druhy podle jejich původu a vlastníka. Rozeznáváme tedy 1st party a 3rd party cookies. Vlastníkem prvního typu je vždy daná

---

[26] The Information That Is Needed to Identify You: 33 Bits. *The Wall Street journal* [online]. August 4, 2010 [cit. 2012-01-04]. ISSN 00999660. Dostupné z: http://blogs.wsj.com/digits/2010/08/04/the-information-that-is-needed-to-identify-you-33-bits/

[27] I v české literatuře se můžeme poměrně často setkat s anglickým výrazem „web bug" či „web beacon".

[28] PETERKA, Jiří. Cookie. In: *eArchiv*: *archiv článků a přednášek Jiřího Peterky* [online]. 2011 [cit. 2012-04-29]. Dostupné z: http://www.earchiv.cz/a96/a638k130.php3

webová stránka, která je ukládá do počítače pouze kvůli vzájemné identifikaci při příští návštěvě nebo pro uložení preferovaného nastavení. Vlastníkem druhého typu jsou naopak třetí strany. Cookies uložené[29] těmito společnostmi pak mohou identifikovat uživatelův počítač na všech webech spravovaných danou agenturou napříč internetem (tzv. cross site tracking) a bez jeho vědomí tak sledovat jeho pohyb. Tyto soubory často ukládají také informace o poslední návštěvě dané stránky nebo o tom, co konkrétně na webu prohlížel. Tímto způsobem pak firmy získávají dostatečné množství údajů potřebné k zjištění zájmů a následnému sestavení profilu. Cookies primárně neobsahují osobní informace, jejichž prostřednictvím by mohly být určena identita uživatele, ovšem jen za předpokladu, že takové informace webové stránce sám neposkytl[30]. V takovém případě může dojít při spojení vytvořeného zájmového profilu s reálnou identitou k zásahu do soukromí.

Local shared object – „Flash cookies“

Local shared object (LSO) je druh cookies souborů, který do počítače ukládají aplikace založené na platformě Flash od firmy Adobe (odtud alternativní název flash cookies). Flash umožňuje využití interaktivních grafických animací, bannerů, přehrávání videí či hraní jednoduchých online her na webových stránkách, bez ohledu na použitý prohlížeč (za předpokladu, že je nainstalován zásuvný modul Adobe Flash Player). Flash cookies by měly mít na starosti obdobné činnosti, jako standardní HTTP cookies, tedy identifikaci, na jejímž základě provede flash aplikace patřičné nastavení. Přesto více než polovina webů používá tyto cookies ke sledování aktivit uživatelů[31].

Oproti standardním souborům cookies mají podle Daniela Dočekala[32] ještě několik negativních vlastností, které uživateli stěžují jejich kontrolu. Běžné mazání cookies souborů prostřednictvím internetového prohlížeče nemá na flash cookies žádný vliv a vzhledem k jejich neomezené expirační době tak mohou zůstat uložené v uživatelově počítači velmi dlouhou dobu. Ukládají také mnohonásobně více dat – až 100 KB oproti 4 KB a nejsou vázané na konkrétní prohlížeč, čímž dovolují třetím

[29] Na cizích stránkách se cookies třetích stran ukládají například prostřednictvím reklamních bannerů.
[30] Slovníček nejdůležitějších pojmů. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ [online]. 2012 [cit. 2012-04-29]. Dostupné z: http://uoou.cz/uoou.aspx?menu=281&loc=455
[31] DOČEKAL, Daniel. Flash Cookies - vlezlé, obtížně smazatelné a masově zneužívané. *Pooh* [online]. 16.8.2010 [cit. 2012-04-29]. Dostupné z: http://www.pooh.cz/IT/a.asp?a=2016280
[32] DOČEKAL, ref 31.

stranám sledovat pohyb uživatele nejen napříč weby, ale i prohlížeči. Některé soubory flash cookies také dokážou obnovit již smazané HTTP cookies bez uživatelova vědomí.

3.1.2. Pixelový tag

Pixelovým tagem je myšlen malý (obvykle o velikosti 1 na 1 pixel) transparentní obrazový soubor, umístěný ve zdrojovém kódu webové stránky nebo e-mailové zprávy[33]. Jeho původcem mohou být opět daná webová stránka nebo vzdálený web třetí strany. V momentě, kdy uživatel otevře webovou stránku opatřenou takovýmto tagem, vyšle prohlížeč na tento pixelový obrázek požadavek na server, ze kterého pochází. Prostřednictvím tohoto požadavku získá vzdálený server od prohlížeče potřebné údaje[34] - IP adresu počítače, ze kterého požadavek vzešel, přesné datum a čas, URL adresu stránky, na které je pixel vložen a informace o prohlížeči. V případě, že má web, ze kterého pixel pochází již v počítači uložené soubory cookies, načte jejich předchozí hodnotu a zaznamená informaci o této relaci. Jelikož má většina uživatelů od poskytovatele připojení přidělenou dynamickou IP adresu, která se mění, nemůže web bug bez jednoznačného identifikátoru počítače uživatele sledovat napříč relacemi. K tomu jsou opět využívány soubory cookies, které mohou být prostřednictvím webového bugu, stejně jako skrze reklamní bannery, uloženy ze zdrojového webu. Některé pixelové tagy také umožňují přesné sledování jednotlivých aktivit na dané stránce, včetně toho, co uživatel píše, či jak pohybuje kurzorem polohovacího zařízení[35].

3.1.3. Pluginy sociálních sítí

Poměrně novým trendem v získávání přehledu o našich internetových aktivitách je využití social-pluginů jednotlivých sociálních sítí. Tyto aplikace a widgety[36] se dnes

---

[33] V e-mailové korespondenci se využívá pro zjištění, zda byla doručená zprávy skutečně otevřena. Tento postup používají například rozesilatele spamu, kteří jeho pomocí ověřují, zdali jsou e-mailové schránky aktivní a má smysl na ně nevyžádanou poštu dále zasílat.

[34] SMITH, Richard M. The Web Bug FAQ. In: *Electronic Frontier Foundation*: *Defending your rights in the digital world* [online]. November 11, 1999 [cit. 2012-04-29]. Dostupné z: http://w2.eff.org/Privacy/Marketing/web_bug.html

[35] ANGWIN, ref. 21, 24

[36] Jedná se o malé nástroje (tlačítka, ikony atd.), reprezentované obvykle javascriptovým kódem či flashovým objektem, vloženým do zdrojového kódu stránky, které nabízejí uživatelům na webových stránkách určité funkce navíc. Může se jednat o například o tlačítko k přihlášení odběru pomocí RSS (RDF Site Summary) kanálu či ji zmíněné pluginy sociálních sítí, indikujících počet sdílení a podobně.
MALÝ, Martin. Widgety: Osvěžení pro vaše webové stránky. *Lupa*: *Server o českém internetu*

nacházejí na velkém množství stránek a umožňují propojení jejich obsahu s profilem na sociální síti, formou oblíbení příspěvku, jeho komentováním či sdílením. Typickým příkladem jsou tlačítka „Like“ sociální sítě Facebook, „+1“ sítě Google+ či „Tweet“ sítě Twitter.

Americký deník USA Today zveřejnil článek[37], ve kterém popisuje, jak přesně takovéto sledování funguje u sociální sítě Facebook. Tato síť prostřednictvím social pluginů sleduje nejen své uživatele, kteří jsou v danou chvíli aktivně přihlášeni, ale také ty odhlášené a dokonce i uživatele, kteří nemají ani založený účet. Ke sledování stačí, aby uživatel alespoň jednou navštívil jednu z domén Facebook.com, která vygeneruje a uloží soubor cookies[38]. Pokud se rozhodne pro vytvoření profilu, Facebook uloží dvoje cookies – cookies prohlížeče (browser) a dočasné cookies (session). Pokud se rozhodne účet nezaložit, uloží se pouze typ browser. Oba typy slouží pro sledování a zaznamenávání pohybu na všech stánkách obsahujících některý z widgetů, liší se však typem informací, které ukládají. Všem uživatelům bez rozdílu uloží navštívené stránky do souboru browser cookie unikátní data (IP adresa, informace o operačním systému a údaje o prohlížeči[39], časové údaje obsahující každou navštívenou URL adresu doplněnou o datum a přesný čas její návštěvy a unikátní (ale anonymní) alfanumerický kód. U aktivně přihlášených uživatelů je místo unikátního kódu využita session cookies, která přidá osobní data z uživatelova profilu – e-mailovou adresu, seznam přátel či jeho záliby. Facebook tedy spojuje výsledky sledování s konkrétními osobami. Podle vyjádření mluvčího Facebooku Andrew Noyese[40] však firma tyto údaje nevyužívá ani pro cílení reklamy ani pro následný prodej třetím stranám. Nicméně v případě úniku

---

[online]. 19. 8. 2009 [cit. 2012-01-04]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/widgety-osvezeni-pro-vase-webove-stranky/

37 ACOHIDO, Byron. Facebook tracking is under scrutiny. *USA today* [online]. 11/15/2011 [cit. 2012-05-01]. ISSN 0161-7389. Dostupné z: http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1

38 Pokud uživatel doménu nenavštíví, či následně vymaže cookies, Facebook nemá možnost ho tímto způsobem sledovat. Například u sociální sítě Twitter však není k uložení identifikačního souboru potřeba navštívit její web; Twitter ho vytvoří a uloží prostřednictvím samotných pluginů.

39 Jedná se o takzvaný otisk prohlížeče (browser fingertprint), který obsahuje informace o použitých fontech, typu a verzi prohlížeče, používaných doplňcích, časové zóně či rozlišení obrazovky. Spojením těchto údajů může vzniknout unikátní otisk daného prohlížeče. Otestovat unikátnost prohlížeče a zjistit, jaké informace o sobě poskytuje lze pomocí projektu online testeru Panoptclick od nadace Electronic Frontier Foundation na adrese: https://panopticlick.eff.org/

40 ACOHIDO, ref. 37.

těchto dat může dojít (zejména v případě aktivně přihlášených uživatelů) k vážnému narušení soukromí uživatelů.

3.2. Krádež identity

Na začátek této podkapitoly je nutné definovat pojem „osobní údaje“. Osobními údaji jsou podle zákona č. 101/2000 Sb., o ochraně osobních údajů[41]: *„jakékoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“*. Nejedná se tedy pouze o údaje typu jména, příjmení či rodného čísla, které obvykle lidé za osobní považují, ale i jakékoliv jiné, které mohou pomoci, přímo či nepřímo, určit jejich identitu.

Krádeží identity není myšleno pouze zcizení osobních dokladů, ale jakékoliv shromažďování a využívání cizích osobních i neosobních[42] údajů, jejichž prostřednictvím se útočník vydává za jinou osobu, za účelem podvodu nebo jiné trestné činnosti[43]. Z právního hlediska se jedná o dvoustupňový trestný čin, který zahrnuje následující fáze[44]:

- samotné získání osobních údajů (identity theft)
- následné zneužití neoprávněně nabytých údajů (identity fraud)

Motivů pro krádež osobních informací je několik. Při získání dostatečného množství údajů se může pachatel vydávat za oběť, ve snaze využít či poškodit její reputaci. Reálné je také riziko zneužití zcizené identity pro podvod pomocí metod sociálního inženýrství. Hlavním důvodem je ale ve většině případů finanční zisk, a to buď přímý (platby prostřednictvím zcizených bankovních účtů), či nepřímý (prodej

---

41 Česko. Zákon ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000. Dostupné z: http://www.uoou.cz/files/101_cz.pdf

42 Ke krádeži identity mohou také posloužit informace, které nejsou podle zákona osobními údaji, např. přihlašovací jméno a heslo k určitým službám.

43 FEDERAL TRADE COMMISSION. *About Identity Theft*: *Deter. Detect. Defend. Avoid ID Theft* [online]. 2012 [cit. 2012-05-01]. Dostupné z: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

44 Krádež identity a jak se jí bránit. *Bezpečný internet* [online]. [cit. 2012-05-01]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

informací třetím stranám). Od toho se odvíjí druhy dat, která jsou nejčastějším cílem těchto útoků. Těmi jsou údaje o kreditních kartách, přihlašovací údaje k e-mailovým schránkám, účty u předplacených služeb, aktivní e-mailové adresy, sloužící pro zasílání spamu apod.

Jak dokazují různé průzkumy, lidé často ochotně sdělují osobní a citlivé údaje cizím osobám výměnou za přislíbenou výhodu. Příkladem může být průzkum provedený v roce 2005 ve městě Los Angeles, při kterém byla náhodným kolemjdoucím nabízena poukázka na kávu v hodnotě 3 dolarů výměnou za některé z jejich přístupových hesel. Celých 180 z 272 dotázaných lidí (tedy více jak dvě třetiny) bylo ochotno své heslo za cenu tří dolarů sdělit. V „druhém kole“ byla lidem, kteří odmítli, nabídnuta ta samá poukázka za prozrazení alespoň podoby hesla; tu prozradilo 51 lidí. Tedy pouze 41 z 272 lidí neprozradilo žádné podrobnosti o svém heslu[45]. Druhým příkladem pak v mnoha variantách opakovaný test s žádostmi o přátelství na sociálních sítích. Zde se jedná o průzkum redakce Technet.cz, která vytvořila falešné profily dívky a chlapce na síti Facebook a jejich prostřednictvím požádala o přátelství (a tím pádem i přístup k citlivým datům) 100 náhodně vybraných uživatelů. Žádost ženského profilu přijalo 60 % chlapců; žádost pánského profilu pak 42 %[46]. Stejně se pak uživatelé chovají v prostředí internetu, kde je dobrovolně vydávají při každé registraci, která jim zaručí „bezplatné“ využití té či oné služby. Co si uživatelé neuvědomují je, že služba ve skutečnosti není zdarma, jelikož cenou za její využívání jsou právě získané osobní informace. Při množství takovýchto služeb, které dnes běžný uživatel denně využívá (ať už se jedná o sociální sítě, freemaily, diskusní fóra či e-shopy), není již v jeho silách uhlídat, kde všude jsou jeho údaje uloženy a jak je s nimi nakládáno. Databáze osobních údajů se pak mohou stát terčem hackerů, kteří jsou do nich schopni proniknout a získat tak velké množství dat. Tato data jsou následně prodávána na černých trzích za nemalé sumy. Hackeři z různých aktivistických skupin často využívají takto získaná a následně zveřejněná data jako projev nesouhlasu (a demonstraci síly) s jednáním určitých

[45] BITTO, Ondřej. Hesla na prodej. *Lupa*: *Server o českém internetu* [online]. 18. 5. 2005 [cit. 2012-01-04]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/hesla-na-prodej/

[46] KASÍK, Pavel. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. *Technet*: *Technika kolem nás* [online]. 19. listopadu 2009 [cit. 2012-05-01]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka

subjektů – organizací, firem, vládních stran apod. Příkladem může být nedávná akce české odnože skupiny Anonymous, která v rámci boje proti schválení dohody ACTA získala a zveřejnila osobní údaje 2731 členů Občanské demokratické strany, včetně jmen, příjmení, adres, rodných čísel, e-mailů, stranických údajů a mnoho dalších[47]. Takovéto útoky jsou však realizovány pomocí složitějších metod, jež vyžadují velké množství znalostí a potřebný výpočetní výkon a mohou být prováděny jen zkušenějšími hackery.

Mnohem větší riziko tak představuje množství nedostatečně zabezpečených či plně přístupných informací, které uživatelé dobrovolně nahrávají a sdílejí, zejména prostřednictvím sociálních sítí. Jelikož nemají tyto sítě žádný zájem chránit soukromí svých uživatelů nad rámec uložený zákonem, bývá mnoho položek jejich účtů (včetně těch obsahujících citlivé informace) primárně nastaveno jako veřejné. Pokud uživatel nepřistoupí k vlastnoručnímu nastavení parametrů zabezpečení soukromí, zůstává jeho profil volně vyhledatelný a veřejně přístupný. A tudíž zneužitelný. Tento přístup umožňuje snadné získání mnoha dat, bez potřeby jakýchkoliv odborných znalostí.

Při možnostech dnešní výpočetní techniky a softwaru je téměř nevyhnutelné, aby se tato data stala terčem automatického dataminingu, realizovaného pomocí šikovně napsaného skriptu či programu. Jak snadný je takový hromadný sběr informací z veřejných profilů na síti Facebook v praxi, předvedl v roce 2010 Ron Bows, který pomocí vlastnoručně vytvořeného kódu získal z veřejné databáze jména a ID čísla více než 100 000 000 uživatelů. Ty pak uložil do samostatného souboru, který nahrál na web Pirate-Bay, kde si ho během chvíle stáhlo více než 1 000 uživatelů[48]. Ron Bows však nezískal (nebo možná pouze nezveřejnil) žádné osobní informace z jednotlivých účtů, ani údaje, které by nebyly běžně dohledatelné, ale poukázal tak na lehkost využití této metody pro hromadný sběr dat. Fakt, že jediný člověk, který chtěl pouze upozornit na problémy ochrany soukromí, nezískal osobní informace z těchto profilů, neznamená, že se firmy či specialisté s využitím jiného kódu k těmto datům nedostanou.

---

[47] DOČEKAL, Daniel. Hacknutý web ODS a data o členech z něj získaná podruhé. *Pooh* [online]. 2.4.2012 [cit. 2012-05-01]. Dostupné z: http://pooh.cz/pooh/a.asp?a=2017672

[48] EMERY, Daniel. Details of 100m Facebook users collected and published. *BBC News* [online]. 29 July 2010 [cit. 2012-01-04]. Dostupné z: www.bbc.co.uk/news/technology-10796584

Se stejným problémem se potýká i sociální síť Google+, jež prostřednictvím webu Google profiles[49] umožňuje vyhledávat v profilech uživatelů. Ty lze samozřejmě, stejně jako u konkurenční sítě Facebook, nastavit jako neviditelné a zamezit tak většině vyhledávačů jejich nalezení[50]. Jelikož se však nejedná o primární nastavení, je mnoho profilů stále volně k dispozici. Toho využil nizozemský student Matthijs Koot, který nechal vlastnoručně napsaný programu projít veřejné účty 35 000 000 uživatelů. Přitom zjistil, že 40% z nich (tedy přibližně 14 000 000) obsahuje uživatelské jméno v podobě e-mailové adresy[51]. Tímto způsobem může útočník za krátkou dobou a s relativně malým úsilím získat celkem rozsáhlou databázi e-mailových adres či jiných osobních údajů, které lze zneužít.

Digitální stopy však nemusí být pouze cílem útoků, ale mohou se stát také prostředkem k jejich realizaci. Bezpečnostním rizikem jsou takzvané kontrolní otázky, které mnoho služeb stále používá jako ověření uživatele pro přístup při zapomenutém heslu. Obvykle se jedná o velmi obecné otázky, jak předvedu na příkladu e-mailové schránky od společnosti Centrum. Ta nabízí celkem 11 otázek typu: *oblíbená filmová postava, oblíbený herec, oblíbený seriál / film, oblíbené / neoblíbené jídlo* či *hudební interpret*. Je jasné, že nalézt odpovědi na takto položené otázky a získat tak přístup k danému účtu, nemusí být, zejména u uživatelů, kteří mají volně dostupný profil na sociální síti, svůj blog či stránku, velký problém. Mnoho z nich totiž dává na sociálních sítích prostřednictvím skupin a stránek najevo svou oblibu toho či onoho produktu / hudebníka / herce apod. Nejedná se samozřejmě o bezpečnostní problém, který by mohl být masově zneužit[52], uvádím ho zde navíc jako zajímavý způsob, jakým mohou být digitální stopy využity.

---

49 https://profiles.google.com/

50 I ke skrytému profilu je však možné se dostat, například přes profily přátel, nastavené jako vyhledatelné, u kterých je takový profil zobrazen v seznamu přátel jako hypertextový odkaz.

51 DOČEKAL, Daniel. Google Profiles nabízejí miliony jmen i e-mailů uživatelů. *JustIT* [online]. 26/05/2011 [cit. 2012-05-01]. Dostupné z: http://www.justit.cz/wordpress/2011/05/26/google-profiles-nabizeji-miliony-jmen-i-e-mailu-uzivatelu/

52 Většina lidí tento způsob ochrany proti ztrátě přístupu nevyužívá a při počtu 11 možných otázek se šance na úspěch také snižuje, jelikož služba nejspíše potencionálního útočníka nenechá vyzkoušet postupně všechny možné otázky. Tento postup by tak mohl být uplatněn zejména při konkrétním cíleném útoku.

3.3. Využití digitálních stop v personalistice

S rozmachem sociálních sítí, který přineslo především spuštění sítě Facebook v roce 2004, získali zaměstnavatelé nový zdroj volně dostupných informací o stávajících zaměstnancích i nových uchazečích o místo v jejich firmě. Uživatelé o sobě prozrazují prostřednictvím sociálních sítí a blogů své zájmy, názory, příslušnosti k určitým skupinám, pracovní reference či fotky z volnočasových aktivit. Z takovýchto informací, tvořících aktivní digitální stopu uživatele, si mohou zkušení HR[53] manažeři a personalisté sestavit portrét uchazeče dříve, než se dojde k prvnímu osobnímu kontaktu. K doplnění portrétu mohou využít také příspěvky v diskuzích a další druhy interakce s ostatními uživateli, ze kterých lze do jisté míry rozpoznat uchazečovy vyjadřovací schopnosti, vzorce chování, rozsah znalostí[54] či schopnost logicky argumentovat. Personalisté dále pátrají po jakékoliv informaci, která by mohla ovlivnit uchazečovo přijetí. Příkladem mohou být fotky z divokých večírků, nenávistné a sprosté komentáře nebo například členství v organizaci propagující rasovou nesnášenlivost. Uživatel by tak měl mít na paměti, že internet „nezapomíná“ a jednou zveřejněné informace nelze vzít jen tak zpět.

Jak cenným zdrojem informací tyto sítě jsou, dokazují statistiky společnosti Reppler, zabývající se monitoringem sociálních médií. Ta provedla v roce 2011 průzkum[55] mezi více než 300 specialisty na personalistiku, s cílem zjistit, jak využívají sociální sítě při výběru uchazečů. Z výsledků vyplývá, že celých 91 % personalistů prověřuje uchazeče pomocí jejich digitálních stop na sociálních sítích. Nejvíce je k tomuto účelu využívána síť Facebook (76 %), kterou následuje síť Twitter[56] (53 %) a pro personalistické účely vytvořený LinkedIn (48 %); sociální síť Google+ nebyla

---

53 HR – Human Resources (lidské zdroje)

54 JANČA, Jan. Sociální sítě a lidské zdroje. *Cognito*: *Prozraďte světu, kdo jste* [online]. 29. 12. 2008 [cit. 2012-05-01]. Dostupné z: http://www.cognito.cz/internet/socialni-site-lidske-zdroje/

55 SWALLOW, Erica. How Recruiters Use Social Networks to Screen Candidates: Infographic. *Mashable*: *The Social Media Guide* [online]. October 23, 2011 [cit. 2012-01-01]. Dostupné z: http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/

56 V českém prostředí nemá sociální síť Twitter tak významné postavení jako ve světě. Podle serveru Klábosení, který se českým Twitterem zabývá, je ke dni 1. 4. 2012 v České republice a na Slovensku dohromady 97 179 uživatelů. Ve většině případů se také jedná o uživatele pohybující se v oblasti sociálních médií či informačních technologií.
Vývoj počtu uživatelů. ATAXO. *Klabosení*: *Český a slovenský Twitter v číslech* [online]. 2012 [cit. 2012-05-01]. Dostupné z: http://www.klaboseni.cz/vyvojpoctu.php

ještě v době průzkumu spuštěna. 69 % dotázaných specialistů někdy odmítlo uchazeče na základě informací, které získali z jejich profilu na sociální síti. Jako nejčastější důvod uvádějí nepravdivé údaje o kvalifikaci, vkládání nevhodných komentářů a fotografií, špatné vyjadřování o předchozím zaměstnavateli, chabé komunikační dovednosti či materiál zachycující požívání alkoholu nebo drog.

Po opadnutí počáteční euforie z nových možností si uživatelé začínají uvědomovat rizika přílišného sdílení osobních informací a zájmů prostřednictvím sociálních sítí. Čím dál častěji tak přistupují k různým formám omezení přístupu k obsahu svého účtu[57]. Některé firmy v USA, které tyto sítě využívají při personálním řízení, se ale s tímto faktem nechtějí smířit. V poslední době bylo zaznamenáno několik případů[58], kdy zaměstnavatel požadoval při pohovoru po uchazečích přístupové údaje (a tudíž prakticky neomezený přístup) k jejich osobnímu účtu na sociální síti Facebook, který byl primárně nastaven jako neveřejný. V případě, že by zaměstnavatel od uchazeče heslo opravdu získal, měl by přístup i k informacím, které nijak nesouvisí s kvalifikací pro dané místo. Uchazeč by však nevystavil riziku zneužití informací pouze sebe, ale také všechny své „přátele". Na tuto kauzu reagoval kromě mnoha expertů i samotný Facebook. Erin Eganová, která má u největší sociální sítě na starosti otázku soukromí, uvedla v prohlášení[59], že tento postup ohrožuje soukromí uživatelů i jejich přátel a vystavuje zaměstnavatele riziku žaloby, jelikož vyžadování a sdílení hesel je v rozporu s podmínkami používání služby Facebook.

Platí nepsané pravidlo, že na internetu by uživatelé neměli dělat (říkat, sdílet) nic, co by neudělali ve skutečnosti. Někteří lidé dnes již začínají chápat, že chování v online prostředí utváří obraz jejich identity stejně, jako je tomu v reálném životě. Z tohoto důvodu stále více lidí kontroluje a upravuje své volně dostupné informace a pomalu přechází k cílenému budování své digitální identity a její dobré pověsti.

---

[57] MADDEN, Marry. *Privacy management on social media sites*. Washington, D.C.: Pew Research Center's Internet & American Life Project, 2012. Dostupné z: http://pewinternet.org/~/media//Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf

[58] V USA chtějí po zájemcích o práci heslo k Facebooku. *E15*: *Ekonomika, byznys, finance* [online]. 24.3.2012 [cit. 2012-05-01]. ISSN 1213-7693. Dostupné z: http://zpravy.e15.cz/byznys/technologie-a-media/v-usa-chteji-po-zajemcich-o-praci-heslo-k-facebooku-754670

[59] V USA chtějí po zájemcích o práci heslo k Facebooku. *E15*: *Ekonomika, byznys, finance*, ref. 58.

4. Možnosti kontroly

Velmi zjednodušeně můžeme říci, že nejlepším způsobem, jak se vyhnout zanechání digitální stopy, je nevyužívat moderní komunikační technologie a internet. Ale v době masové elektronizace různých lidských činností, kdy většina lidí ve vyspělých zemích využívá tyto technologie i k nejběžnějším úkonům každodenního života si lze tento postup jen stěží představit. Ačkoliv existuje mnoho metod a nástrojů, kterými uživatelé mohou chránit své soukromí v online prostředí, nemůže ani jejich využití zajistit stoprocentní ochranu před vznikem digitálních stop. Lze tak předpokládat, že každý běžný uživatel nějakou svou stopu již má. Otázkou tedy není, zdali stopu má, ale jak jeho stopa vypadá.

4.1. Možnosti zjištění rozsahu digitální stopy

Aktivní stopy

Nejjednodušším způsobem, jak může uživatel získat přehled o rozsahu své (především aktivní) digitální stopy, je tzv. „egosurfing“[60]. Jde o využití obyčejného vyhledávače pro zobrazení dostupných informací a dat spojených s uživatelovým jménem. K rozšíření výsledků vyhledávání a získání přesnějšího obrazu lze doplnit i jiná data (např. e-mailovou adresu, přezdívku, školu), která mohou vést k jeho identifikaci.

4.1.1. People search engines

Egosurfing není v dnešní době nic neobvyklého; k využití vyhledávačů pro nalezení informací o své osobě někdy přistoupilo na 47 % dospělých Američanů, 3 % z nich provádějí takovéto hledání pravidelně, 22 % jednou za čas a zbylých 74 % pouze jednou nebo dvakrát[61]. Z tohoto důvodů vzniklo[62] mnoho samostatných vyhledávačů, uzpůsobených právě k vyhledávání lidí (a s nimi souvisejících informací), tzv.„people search engines“, které mohou být alternativou k běžným vyhledávačům.

---

[60] Tento termín poprvé použil Sean Cartonv roce 1995 ve svém sloupku Jargon watch v časopise Wired, a v roce 2011 byl dokonce přidán do Oxfordského slovníku (Oxford English Dictionary), jednoho z nejvýznamnějších slovníků anglického jazyka.
Egosurfing. In: *Techopedia*: *The IT Education Site* [online]. c2010 - 2012 [cit. 2012-05-05]. Dostupné z: http://www.techopedia.com/definition/26356/egosurfing

[61] MADDEN, ref. 14

[62] Zejména v Severní Americe; jejich funkce jsou tedy pro hledání lidí např. z České Republiky omezené, přesto však dokážou nalézt množství informací.

Nejviditelnějším znakem tohoto uzpůsobení spočívá v zobrazování výsledků vyhledávání, které nemá formu seznamu hypertextových odkazů, ale komplexního přehledu nalezených informací. Na jedné stránce tak uživatel nalezne dostupné informace roztříděné podle kategorií (obvykle vytvořených podle zdroje dat), tedy např. výsledky hledání na sociálních sítích, nalezené e-mailové kontakty, veřejné záznamy, domény, blogy, obrázky, videa, dokumenty, záznamy z kriminalistické databáze či dokonce vazby na příbuzné osoby. Oproti běžným vyhledávačům obvykle nabízejí i některé funkce, umožňující zvýšit počet nalezených informací. Proto zde uvedu dva příklady takovýchto vyhledávačů, jež nabízejí uživateli něco více, než vyhledávače klasické.

Pipl

Pipl patří mezi nejznámější people search enginy. Využívá svůj vlastní algoritmus, který je schopný proniknout a prohledat i tzv. hluboký web, tedy tu část internetu, kterou roboti běžných vyhledávačů nejsou schopni (nebo nechtějí) z nějakého důvodu zanést do svých indexů a nejsou tak schopné v něm vyhledávat[63].

People Finders

Peple Finder nabízí svým uživatelům kromě běžných zdrojů vyhledávání také databázi kriminálních záznamů (platí pouze pro USA), v níž lze zjistit podrobnosti o kriminální minulosti hledané osoby, včetně posouzení úrovně rizika v případě sexuálních delikventů. Dalšími známými people search enginy jsou např. Zabasearch, Spock, 123people či Spokeo.

Po odstranění nerelevantních výsledků, které jsou způsobeny například shodou jmen s jinou osobou, může uživatel zhodnotit množství a obsah dostupných informací z hlediska ochrany soukromí či jiných bezpečnostních rizik, promyslet a případně přijmout potřebná opatření pro jejich odstranění.

---

[63] Překážkou mohou být například formuláře, omezení přístupu ze strany vlastníka, dynamicky generované stránky či zvláštní formáty dokumentů. Velikost hlubokého webu nelze s přesností určit, odhaduje se však, že je přibližně 500 x větší než web viditelný. Je tedy jasné, že i když do něj zmíněný algoritmus dokáže proniknout, prohledá jen malou část, například určitý počet vládních databází.
The Ultimate Guide to the Invisible Web. *OEDB*: *Online Education Database* [online]. c2006-2012 [cit. 2012-05-06]. Dostupné z: http://oedb.org/library/college-basics/invisible-web

4.1.2. Facebook information download

Od roku 2010 nabízí největší sociální síť Facebook svým uživatelům možnost získat informace o jejich aktivitách na této síti. Uživatel má na výběr ze dvou druhů archivů, které se liší počtem a typem informací, které obsahují. První je klasický a obsahuje tyto informace[64]:

- informace uvedené v profilu, například kontaktní údaje, zájmy nebo skupiny
- příspěvky na zdi a obsah, který sám uživatel a jeho přátelé umístili do svého profilu
- nahrané fotky a videa
- seznam přátel
- poznámky
- události (na které uživatel odpověděl)
- odeslané a přijaté zprávy
- všechny komentáře, které uživatel a jeho přátelé přidali k příspěvkům na zdi fotkám a dalšímu obsahu profilu

Z výčtu je jasné, že se jedná pouze o kopii uživatelského profilu (jeho stavu aktuálnímu k datu žádosti) a z hlediska získání nových informací o rozsahu dat, která Facebook ukládá, nemá pro uživatele žádný větší význam. Obsahuje tedy pouze aktivní digitální stopu.

Zajímavější je tedy druhá možnost, kterou představuje rozšířený archiv. Ten obsahuje data ukládaná v pozadí, zachycující průběh interakcí uživatele s Facebookem a zachycuje tak i jeho stopu pasivní. Tento archiv může obsahovat například[65]:

- IP adresu – výčet všech IP adres, které Facebook uložil (nejedná se však o výčet všech adres, které kdy měly přístup k danému účtu)
- přihlašovací informace - seznam uložených přihlášení (opět se nejedná o všechna přihlášení za celou historii účtu)

---

[64] Stahování informací. FACEBOOK. *Centrum nápovědy* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.facebook.com/help/?page=116481065103985

[65] FACEBOOK, ref. 64.

- odhlašovací informace - IP adresy, ze kterých proběhla odhlášení
- čekající žádosti o přátelství - odeslané žádosti o přátelství a žádosti obdržené, které byly ignorovány či zamítnuty
- změny stavu účtu - data, kdy byl účet opět aktivován, deaktivován, vyřazen z provozu nebo odstraněn
- informace o šťouchání
- informace o událostech - události na které uživatel reagoval (tzn. označil jednu z možností ano / ne / možná)
- další informace o profilu (pouze za předpokladu, že uživatel vyplnil)
    - čísla mobilních telefonů
    - město a rodné město
    - jména členů rodiny
    - informace o vztazích (všechny minulé vztahy včetně jmen osob, se kterými byl uživatel ve vztahu)
    - seznam jazyků
    - historie veškerých změn uživatelského jména

Zde se již jedná o data zajímavějšího charakteru, jež na rozdíl od informací z prvního balíčku poskytují uživateli náhled do pozadí jeho počínání na této sociální síti.

Ačkoliv by se mohlo zdát, že se jedná o zajímavý nástroj, prostřednictvím kterého mohou mít uživatelé přehled o svých informacích a mohou tak nad nimi získat lepší kontrolu, není tomu tak. Důvodem jejího spuštění je reakce na stížnost rakouského studenta práv Maxe Schremse, který ve své školní práci poukázal na jisté problémy se zpracováním a uchováváním, které jsou v rozporu s evropskými předpisy. V souladu s evropskou legislativou 95/46/ES o ochraně osobních údajů[66] zaručující uživatelům právo na přístup k informacím, které jsou předmětem zpracování, si vyžádal kompletní výpis informací, jež o něm Facebook ukládá. Jako odpověď získal CD, obsahující na 1222 stran dat zaznamenávající veškerou jeho činnost na této sociální síti. Zjistil tak například, že veškerá data, včetně smazaných, jsou stále uložena na serverech

[66] Evropská Unie. Směrnice Evropského parlamentu a Rady 95/46/ESze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *Úřední věstník evropských společenství*. 23.11.1995. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:CS:PDF

Facebooku (pouze s připojenou poznámkou „deleted“ - smazáno) a jejich odstranění znamená pouze zneviditelnění pro uživatele. Max Schrems založil iniciativu Europe - v - Facebook[67], kde ostatním uživatelům ukazuje, jaká data jsou o nich ukládána a jak je mohou sami získat.

I když rozšířený archiv obsahuje množství informací, ani zdaleka nedosahuje objemu kompletního výpisu, který lze získat oficiální cestou s odvoláním na evropské zákony. Schrems uvádí[68], že tento relativně lehce získatelný archiv obsahuje (v závislosti na počtu informací uvedených v profilu) pouze okolo 29 % celkového počtu informací, které Facebook schraňuje. Facebook information download je tedy spíše nástroj, jak dát uživateli pocit kontroly nad svými informacemi a vyhnout se tak povinnosti vydávat v případě žádosti kompletní přehled. Jelikož se jedná o závaznou evropskou směrnici, může uživatel využít tohoto práva a dožadovat se svých informací u jakéhokoliv subjektu podnikajícího na území Evropské unie.

4.1.3. Google Dashboard

Google Dashboard je užitečný nástroj, s jehož pomocí může uživatel spravovat svou online identitu u více než dvaceti nejvyužívanějších služeb, které Google nabízí (Gmail, kalendář, dokumenty, historie, Youtube, Google+ apod.), z jednoho místa. S tímto prostředkem uživatel získá komplexní přehled o využívaných službách a množství a druhu osobních informacích, které jsou jejich prostřednictvím dostupné.

Kromě této funkce nabízí také možnosti upravení soukromí u jednotlivých služeb či rady a nástroje, jak nechtěné informace odstranit. Jelikož se jedná o velmi rozsáhlý nástroj, zmíním jednotlivé funkce i v následujících kapitolách, do kterých lépe zapadají.

Pasivní stopy

U pasivních digitálních stop jsou šance na jejich odhalení mnohem menší, než u stop aktivních, a to i přes výše zmíněný zákon umožňující uživatelům získat přehled o svých datech. Hlavním příčinou je skutečnost, že ačkoliv je v dnešní době sledování

[67] http://europe-v-facebook.org/

[68] Get your Data: Make an Access Request at Facebook!. *Europe-v-Facebook* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html

návyků třetími stranami obecně známým faktem, běžní uživatelé stále nemají o těchto metodách téměř žádné povědomí, nepovažují je za riziko a nepřijímají proto patřičná opatření, aby své soukromí lépe chránili. Vzhledem k velkému počtu sledovacích zařízení, která obsahují jednotlivé weby, je velmi obtížné (ne-li přímo nemožné) získat zpětně přehled o všech možných firmách, které by mohly vlastnit uživatelův profil získaný jejich prostřednictvím. Se stejným problémem se bude uživatel potýkat i v případě osobních údajů zadaných při registraci do různých online služeb či při nákupech skrze e-shopy, které ji v mnoha případech vyžadují. I ve velmi nepravděpodobném případě, že by se uživateli povedlo identifikovat všechny subjekty, kterým kdy mohl při registraci poskytnout své osobní údaje, s největší pravděpodobností se stále nebude jednat kompletní výčet všech subjektů, které mohou tato data uchovávat. Jak jsem již zmínil ve třetí kapitole, stávají se osobní data na internetu cenným artiklem, se kterým se běžně obchoduje. Zjistit, kam až se data při těchto transakcích dostala, je pro běžného uživatele nemožné.

4.1.4. Google Ad Preferences

Ad Preferences od společnosti Google je nástroj, jehož účelem je pomoci uživateli získat a upravit informace, které Google používá pro doručování cílené reklamy na webech své reklamní sítě. Uživatel si tak může jeho prostřednictvím nastavit své preference tak, aby se mu nadále zobrazovala jen reklamní sdělení, o které má zájem, nebo cílenou reklamu ze strany Googlu úplně zakázat. Z hlediska digitálních stop je tento nástroj zajímavý, jelikož nabízí možnost plného přístupu k behaviorálnímu profilu, sestavenému (a částečně vydedukovanému) společností Google na základě informací získaných sledováním jeho aktivit. Funkčnost této aplikace je však podmíněna dvěma faktory, uživatel musí mít založený účet alespoň u některé ze služeb společnosti Google a musí mít v prohlížeči povolené přijímání cookies souborů třetích stran.

Tento nástroj samozřejmě uživatelům neumožní zjistit plný rozsah jejich pasivní stopy, může však poskytnout zajímavý přehled o tom, jak takový zájmový profil

sestavený reklamními společnostmi vypadá; v tomto případě dokonce u společnosti, která je největším poskytovatelem analýz pro zadavatele reklamy[69].

4.2. Správa digitálních stop

Aktivní stopy

Fakt, že nejlepší ochranou je prevence platí i v případě digitálních stop. Každý uživatel by si měl uvědomovat, že jakékoliv informace a data, která se jednou dostanou na internet, je následně velmi obtížné odstranit a mohou se prakticky kdykoliv znovu objevit a způsobit případné potíže. Nejbezpečnějším způsobem, jak zamezit budoucím problémům s přemírou zveřejněných dat, je tato data jednoduše nezveřejňovat. S tímto přístupem, však uživatel nebude moci využít plného potenciálu webových služeb. Pokud uživatel bude chtít (nebo potřebovat) užívat všech výhod, které internet v dnešní době nabízí, zveřejnění určitého množství dat se nevyhne. Stejný problém pak nastává i v případě stop pasivních.

Základním předpokladem pro snížení potencionálních rizik plynoucích ze vzniku aktivní digitální stopy je dodržování určitých bezpečnostních zásad. Tyto zásady se objevují v mnoha odlišných verzích; pro příklad zde uvedu doporučení z portálu E-bezpečí[70] (která pro úplnost ještě sám doplním, na základě vlastních zkušeností):

- ***Využití více přihlašovacích jmen (přezdívek)*** pro jednotlivé služby, čímž lze do jisté míry zabránit snadnému získání mnoha informací a následnému sestavení profilu uživatele např. pro personalistické účely. Použitá přihlašovací jména by také neměla svým tvarem prozrazovat citlivé informace, které mohou dále usnadnit identifikaci uživatele (např. přezdívka „Martin1987“).

- ***Uvážlivé publikování fotografií, videí a osobních údajů.*** Uživatel by měl velmi pečlivě vybírat jaká data a informace nahrává a zejména prostřednictvím jakých webů či služeb. Na základě podmínek pro užívání a podmínek ochrany osobních

[69] EVIDON, Inc. *Know Your Elements* [online]. c2011 [cit. 2012-05-14]. Dostupné z: http://www.knowyourelements.com/

[70] ČERNÝ, Michal. Digitální stopy. In: *E-bezpečí* [online]. 19.9.2011 [cit. 2012-01-04]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalni-stopy

údajů, které jednotlivé služby mají povinnost zveřejňovat, může uživatel získat přehled, jak bude s jeho daty dále nakládáno. Zda nejsou například předávána třetím stranám či služba nezíská nahráním veškerá práva pro jejich další využití.

- ***Vhodné nastavení soukromí*** u všech služeb (zejména pak sociálních sítí), které tuto možnost nabízejí. Tímto nastavením může uživatel do jisté míry ovlivnit vyhledatelnost dat zveřejněných prostřednictvím těchto služeb, či omezit přístup cizím uživatelům.

- ***Vhodné nastavení zabezpečení prohlížeče.*** Jak vyplývá z kapitoly 3.1, je ke sledování návyků uživatelů napříč internetem, potřeba uložení souboru cookie. Všechny moderní prohlížeče nabízejí možnost správy těchto souborů. Prostřednictvím prohlížeče tak lze blokovat přijímání cookies. Aby však nedošlo k omezení funkčnosti webových aplikací, které by mohlo nastat při omezení všech cookies, je možné blokovat pouze ty, jež pocházejí od třetích stran, či nastavit výjimky pouze pro určité servery. Důležitým krokem je také pravidelná kontrola a mazání již uložených cookies (nevztahuje se na flash cookies), které lze provádět ručně nebo automaticky při každém zavření prohlížeče.

Jelikož jsou však k získávání informací využívány stále složitější nástroje (např. systémy pro rozpoznávání obličejů), je potřeba využít různé nadstavbové nástroje i pro jejich ochranu.

4.2.1. Me on the web

Me on the Web (česky „Já na webu“) je služba realizovaná v rámci již zmíněného nástroje pro správu online identity Google Dashboard. Jedná se tzv. alertovou (monitorovací) službu, jejímž účelem je sledování nových informací v určité oblasti vymezené uživatelem prostřednictvím zadaných klíčových slov. Zde je tento princip využíván pro kontrolu osobních údajů, které se o uživateli objeví ve výsledcích vyhledávání. Pokaždé, když vyhledávací robot odhalí a oindexuje nově zveřejněnou informaci, která se shoduje s nastaveným dotazem, obdrží uživatel o tomto zveřejnění e-mailové upozornění. Uživatel tak získává možnost automaticky kontrolovat informace, které o něm zveřejňují ostatní osoby. Jelikož je však alertová služba, stejně

jako klasický vyhledávač, omezena pouze na viditelný web, nemusí postihnout všechny poskytnout úplný přehled o zveřejněných informacích.

Ve službě Me on the Web jsou upozornění primárně nastavená (nikoliv však aktivovaná) na jméno a e-mailovou adresu, skrze které uživatel přistupuje ke svému účtu. Me on the Web však nabízí možnost vytvořit až pět[71] dalších upozornění na libovolná klíčová slova. Uživatel tedy může do vyhledávání zahrnout například i přezdívky, jiné e-mailové adresy, telefonní čísla či skutečnou adresu, a značně tak rozšířit rozsah zachycených informací. U všech nastavených klíčových slov je možné zobrazit náhled aktuálního stavu informací dostupných ve výsledcích vyhledávání. Zvolit lze také frekvenci zasílání jednotlivých upozornění, a to buď v denním intervalu, týdenním intervalu, a nebo pouze v případě, že objeví nová informace.

Uživatel má možnost využít bezplatné alertové služby také u jiného poskytovatele, například velkých vyhledávačů Yahoo! či Bing. Tyto služby se však v zásadě nijak výrazně neliší a jediným důležitým rozdílem je využití odlišných vyhledávacích algoritmů, které mohou ovlivnit počet nalezených informací. Využitím kombinace více monitorovacích služeb lze tedy zvýšit šanci na získání většího množství relevantních výsledků. Pro ukázku možnosti využití alertových služeb při kontrole digitálních stop tedy postačí pouze příklad společnosti Google. Služba Me on the Web byla vybrána záměrně, jelikož je přímo prezentována jako nástroj správy online identity (ačkoliv v praktickém využití nenabízí, oproti konkurenci, žádné služby navíc).

Pasivní stopy

Pohybovat se v prostředí internetu bez zanechávání jakékoliv pasivní stopy je nemožné. I v případě využití silných metod ochrany je možné teoreticky tuto stopu získat, jelikož všechna zařízení spolu při vzájemné interakci komunikují data a metadata, čemuž nelze nijak zabránit. Existují však způsoby, jakými běžný uživatel může chránit své soukromí před případnými riziky pasivních stop, zejména sledování

[71] V případě, že by uživatel z nějakého důvodu potřeboval zadat více klíčových slov, může využít služby Google Alerts, která funguje paralelně se službou Me on the web a nabízí prakticky totožné funkce.

uživatelských návyků a následnému sestavování a prodeji profilů. Zde uvedu několik příkladů takových nástrojů.

4.2.2. Do not Track

Další možností, jak částečně zamezit nechtěnému sledování, je využití funkce „Do not track“. Při komunikaci se serverem prostřednictvím protokolu HTTP (Hypertext Transfer Protocol) může prohlížeč přidávat pomocí tzv. HTTP hlaviček (headers) informace určující parametry této komunikace. Do not track přidává k této komunikaci HTTP hlavičku ve formátu <*DNT=1*>, jejímž prostřednictvím informuje navštívenou webovou stránku, že si uživatel nepřeje být sledován napříč internetem.

Funkci Do not track nechala vytvořit Federální obchodní komisí (Federal Trade Commision) na žádost několika organizací zabývajících se ochranou práv spotřebitelů (např. World Privacy Forum, Center for Democracy and Technology či Electronic Frontier Foundation). Poprvé byla implementována do čtvrté verze prohlížeče Mozilla Firefox v roce 2011[72]. V současné době je dostupná také u nejnovějších verzí prohlížečů Internet Explorer (Microsoft), Opera (Opera Software) a Safari (Apple). Jediný zástupce velkých prohlížečů Google Chrome zatím tuto možnost nenabízí, měl by ji však zprovoznit nejpozději do konce roku 2012[73].

Problémem tohoto řešení je zejména fakt, že se ze strany uživatele jedná pouze o žádost a neexistuje žádná zákonná povinnost jeho přání respektovat. Implementace a dodržování funkce Do not track je tak závislé pouze na správci dané webové stránky. Zejména velké reklamní firmy, které vydělávají na doručování cílené reklamy, dlouho tuto funkci ignorovaly. V únoru letošního roku však koalice Digital Advertising Alliance sdružující více než čtyři sta reklamních společností oznámila, že v rozmezí devíti měsíců začnou její členové tyto žádosti přijímat a respektovat[74].

---

[72] Mozilla Firefox 4 Beta, now including “Do Not Track” capabilities. MOZILLA. *The Mozilla Blog*: *News, notes and ramblings from the Mozilla project* [online]. February 8th, 2011 [cit. 2012-05-14]. Dostupné z: http://blog.mozilla.org/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/

[73] ANGWIN, Julia. Web Companies Agree to Support 'Do Not Track' System. *The Wall Street journal* [online]. February 23, 2012 [cit. 2012-01-04]. ISSN 00999660. Dostupné z: http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html

[74] ANGWIN, Julia. Web Companies Agree to Support 'Do Not Track' System, ref. 73.

4.2.3. Opt-outs

Opt-out je termín, obecně označující mechanismus, který umožňuje uživateli vyvázání se z nechtěné služby. Opt-out nástroje nabízí většina známých reklamních společností a dovolují tak uživatelům zrušit behaviorální cílení reklamy z jejich strany. Princip této služby spočívá v uložení příslušných informací prostřednictvím souboru cookies, který v případě dalšího kontaktu serveru sdělí, že si uživatel nepřeje cílenou reklamu. Pro správné fungování je tedy potřeba mít v prohlížeči povolené cookies třetích stran, což je ovšem z hlediska ochrany soukromí kontraproduktivní krok. Řešením může být nastavení výjimek pro všechny firmy, z jejichž reklamy se chce uživatel vyvázat, ale při jejich množství by se jednalo o velmi zdlouhavý proces. Navíc vyvázání z dodávání personalizované reklamy podle Setha Schoena, vedoucího technického pracovníka Electronic Frontier Foundation ještě neznamená, že firmy nebudou dále shromažďovat a analyzovat tato data pro jiné účely[75].

Pokud si i přes tyto nedostatky uživatel bude přát využít možnost opt-out, lze tak učinit prostřednictvím některých web i hromadně (u společností, které s daným webem spolupracují). Příkladem mohou být weby Network Advertising Initiative (94 společností), About Ads (101 společností), či do českého jazyka lokalizovaná služba Your Online Choices (57 společností). Přesto, že tyto weby nabízejí relativně velké množství společností, z jejichž služeb se lze vyvázat, stále se jedná pouze o část celkového počtu.

4.2.4. Softwarové řešení

Alternativou k výše zmíněným nástrojům, je řešení pomocí softwarových nástrojů v podobě programů či doplňků prohlížečů (add-ons). Ty na rozdíl od hlaviček Do not Track a mechanismů opt-outs, jež nemusí vždy zabránit sledování návyků a sběru dat, nabízejí aktivní ochranu, jelikož dokážou jednotlivé prostředky pro sledování blokovat. Pro názornou ukázku zde uvedu jeden příklad takového programu; více zástupců pak bude předmětem komparace v praktické části této práce.

---

[75] MARTÍNEZ-CABRERA, Alejandro. Erasing all digital footprints 'impossible'. *San Francisco chronicle* [online]. San Francisco, Calif.: Chas. D. Young, July 6, 2010 [cit. 2012-05-14]. ISSN 1932-8672. Dostupné z: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/07/05/BU4V1E8D9V.DTL

Ghostery

Ghostery je volně stažitelný doplněk pro internetového prohlížeče vytvářený firmou Evidon. V současné době dostupný pro všechny velké prohlížeče – Firefox, Opera, Safari, Internet Explorer i Chrome.

Nástroj funguje na principu tří kroků:

- ***Detect*** *(odhalit)* při kterém nástroj na navštívené webové stránce odhalí a určí původ jednotlivých skrytých sledovacích zařízení, vložených ve zdrojovém kódu stránky.

- ***Learn*** *(poznat)* nabídne uživateli jejich seznam. U každého nalezeného zařízení dává uživateli možnost otevřít profil společnosti, obsahující popis a za jakým účelem je prováděn sběr informací, jaký typ dat je jejich prostřednictvím shromažďován, zda je sdílen s třetími stranami či na jak dlouhou dobu jsou sebraná data následně uchovávána. Nechybí ani odkaz na podmínky ochrany soukromí, dané společnosti. Tento seznam obsahující profily více jak 500[76] různých subjektů, umožňuje uživateli dozvědět se více o jejich fungování a na základě těchto znalostí rozhodnout, zda příslušné sledovací zařízení zablokovat či nikoliv.

- ***Control*** *(kontrolovat)* je posledním krokem, kdy na Ghostery zablokuje skripty uživatelem vybraných sledovacích zařízení a znemožní tak jejich fungování. Tento proces se odehrává bez ohledu na vyjádření vlastnické firmy, jak je tomu u Do not Track. Seznam zablokovaných společností neplatí pouze pro danou stránku, ale napříč všemi weby, kde má umístěná svá monitorovací zařízení.

I když se jedná pouze o doplněk, nikoliv o samostatně stojící software, nabízí Ghostery množství nastavení. Dovoluje tak uživateli například vybrat druh sledovacích zařízení, která mají být blokována, či rovnou zakázat sledování u všech společností v databázi. Zajímavou funkcí navíc je nástroj na odstraňování Flash cookies, na které se nevztahuje běžné odstranění pomocí prohlížeče.

---

[76] Databáze je neustále aktualizována a doplňována o nové společnosti.
About Ghostery. EVIDON, Inc. *Ghostery* [online]. 2011 [cit. 2012-07-30]. Dostupné z: https://www.ghostery.com/about

4.2.5. Anonymní prohlížení

Další možností, jak omezit nechtěné zanechávání stopy při pohybu internetem je využití různých anonymizačních technik, které dokážou skrýt či pozměnit jednotlivé údaje (IP adresa, otisk prohlížeče, HTTP hlavičky) umožňující identifikaci komunikačního zařízení a za jistých okolností tedy i konkrétní osoby. Existuje celá škála různých anonymizačních prostředků, které se liší jak použitou technikou, tak mírou zabezpečení. U většiny těchto prostředků jsou obvykle nabízeny i placené verze, poskytující zpravidla lepší ochranu uživatelovy identity a další výhody jako je vyšší rychlost přenosu dat či možnosti individuálního nastavení. Zde se však budu, s ohledem na téma práce, zabývat pouze volně dostupnými nástroji.

Anonymní módy

Funkce anonymního prohlížení je dnes běžnou součástí webových prohlížečů a můžeme se s ním setkat pod různými názvy „InPrivate Browsing“ (Internet Explorer), „Incognito mode“ (Chrome) či „anonymní prohlížení“ (Firefox, Safari) či „soukromé prohlížení“ (Opera). Všechny však plní stejné základní funkce – zabraňují ostatním uživatelům na daném počítači zjistit historii prohlížení webových stránek a zároveň bránit různým subjektům sledovat pohyb uživatele po internetu. Prohlížeče po ukončení prohlížení v anonymním režimu smažou veškeré záznamy komunikace (historie, cookies apod.), kromě stažených souborů.

Aby bylo možné zabránit jejich prostřednictvím sledování uživatelů, měly by dokonale oddělit veškerou komunikaci vedenou v anonymním módu od komunikace vedené v módu standardním a naopak. Pole studie Stanfordské univerzity[77] však tomu tak není. Ne všechny položky, které zůstávají dostupné v obou módech, představují pro uživatele riziko. Nicméně prohlížeč Safari společnosti Apple umožňuje při anonymním prohlížení webovým stránkám číst a přepisovat soubory cookies uložené v počítači z předchozích relací. Tímto způsobem Safari dovoluje webovým stránkám, které již mají cookies uložené sledovat uživatele bez ohledu na použitý mód. Největším bezpečnostním rizikem, které je v různé míře společné pro všechny prohlížeče jsou

[77] AGGARWAL, Gaurav, Elie BURSZTEIN, Collin JACKSON a Dan BONEH. An analysis of private browsing modes in modern browsers. In: *Proceedings of the 19th USENIX Security Symposium*. Wahington, D.C., 2010, s. 79-94. Dostupné z: http://static.usenix.org/events/sec10/tech/full_papers/Aggarwal.pdf

doplňky (add-ons) a zásuvné moduly (paginy) sloužící k rozšíření funkčnosti jednotlivých prohlížečů. Některé doplňky a zásuvné moduly, které mohou sloužit v běžném režimu ke sledování návyků uživatelů, tyto funkce neztrácí ani při zapnutém privátním prohlížení. Záleží tedy pouze na daném prohlížeči, jak se k takovému riziku postaví. V tomto ohledu selhal prohlížeč Firefox, u nějž nejsou funkce doplňků nijak omezeny. Chrome a Internet Explorer mají v anonymním módu doplňky primárně zakázané, nicméně některé mohou i přesto zůstat aktivní[78]. Prohlížeč Safari pak nepoužívá žádné podporované doplňky a v tomto ohledu tedy nepředstavuje žádné riziko. Z hlediska požadavků na technické znalosti uživatele se tedy jedná o nejjednodušší, zároveň však nejméně účinný způsob zajištění bezpečnosti.

Webové proxy (anonymizéry)

Proxy server je obecně zařízení (např. server, router), s přidělenou veřejnou IP adresu (a tedy schopné přistupovat k internetu) které hraje roli prostředníka při spojení mezi uživatelem a cílovým serverem[79]. IP adresa uživatelova počítače je tedy skryta za IP adresu proxy serveru, který obstarává koncovou komunikaci s cílovým serverem. Nejjednodušší přístup k těmto krycím službám pak nabízejí volně dostupné anonymizéry, tedy webové proxy. Z pohledu uživatelského rozhraní se jedná o běžnou webovou stránku, na které je vložené vyhledávací okno, do kterého stačí vložit URL adresu požadovaného webu a proxy server se již postará o zbytek.

Vzhledem k jednoduchosti tohoto řešení existuje proxy serverů velké množství. Pravidelně aktualizované seznamy dostupných proxy serverů nabízejí různé weby, např. *proxy.org*, *publicproxyservers.com* a mnoho dalších. Uživatel si zde může vybrat server podle lokace, ve které se nachází[80] či podle míry poskytované anonymity (standardní či HiAnon – vysoce anonymní).

Jednoduchost řešení však s sebou přináší několik nevýhod. Některé anonymizéry při komunikaci neblokují HTTP hlavičky, které mohou za jistých okolností prozradit IP adresu uživatele. Druhým problémem je pak důvěryhodnost, jelikož množství těchto

[78] AGGARWAL, ref. 77.

[79] VRBA, Marek. Proxy servery: jak se falšuje návštěvnost. *Lupa*: *Server o českém internetu* [online]. 26.1. 2005 [cit. 2012-01-04]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/proxy-servery-jak-se-falsuje-navstevnost/

[80] Může sloužit například pro přístup k obsahu, který je dostupný pouze v určité zemi.

proxy serverů funguje na virem napadených (a hackery ovládaných) počítačích běžných uživatelů, kteří nic netuší[81]. Takovéto proxy servery pak mohou útočníkům sloužit jako tzv. „honey pots“ a schraňovat citlivé údaje o komunikace, která je skrze ně vedena.

Vícenásobné proxy

Největší možnost ochrany soukromí pak nabízejí nástroje, které směřují komunikaci mezi uživatelem a koncovým serverem přes několik jednotlivých uzlů. Dobrat se zpětně k uživateli, který použil tuto metodu, je téměř nemožné. Mezi nejznámější volně dostupné služby tohoto typu patří projekt TOR a JAP (JonDonym).

TOR

TOR (The Onion Routing – „cibulové směrování“), vznikl v roce 2004 jako projekt Amerického námořnictva, který měl zajistit ochranu vládní komunikace[82]. Nyní se o jeho údržbu a vývoj stará nezisková organizace The Tor Project a služba je volně dostupná pro veřejnost.

TOR pracuje na principu sítě onion routerů, skrze které putuje od uživatele požadavek na koncový server. Uživatel vyšle požadavek na určitou webovou stránku prostřednictvím svého TOR klienta, který data zašifruje do několika vrstev (odpovídající počtu jednotlivých routerů, skrze které data poputují) z nichž každá obsahuje informace o dalším uzlu, na který se mají data poslat, a vybere první router. Ten přijme data, dekóduje (a odstraní) svrchní vrstvu, která obsahovala jeho adresu, čímž odhalí vrstvu další s adresou příštího routeru[83]. Tento proces se opakuje do doby, než na posledním routeru zůstane původní požadavek, který bude jeho prostřednictvím předán na patřičný server[84]. Server tedy předpokládá, že iniciátorem komunikace je právě poslední přístupový bod, čímž zůstane původní uživatel skrytý. Jednotlivé uzly

---

81 TOMEK, Lukáš. Anonymní surfování: na výběr máte z několika možností. *Lupa*: *Server o českém internetu* [online]. 19. 3. 2010 [cit. 2012-01-04]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/anonymni-surfovani-na-vyber-mate-nekolik-moznosti/

82 About Tor: Overview. *Tor Project* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.torproject.org/about/overview.html.en

83 Právě díky principu postupného „odlupování“ jednotlivých vrstev získal tento typ komunikace název „cibulový“.

84 Zde je jediné slabé místo celé sítě. Původní obsah datové zprávy je díky několikanásobnému šifrování dobře chráněn. Poslední router však kvůli postupnému odpadávání jednotlivých vrstev manipuluje již s nešifrovanými daty.

znají pouze adresy sousedních routerů, se kterými bezprostředně komunikují, což velmi ztěžuje identifikaci zařízení, ze kterého požadavek vyšel.

Jednotlivé přístupové body představují obvykle počítače uživatelů - dobrovolníků, kteří svého TOR klienta nastavili jako veřejný uzel a umožnili tak rozšíření sítě. Zde však spočívá největší problém, bránící využití onion routingu v každodenní praxi. Rychlost přenosu dat záleží na každém jednotlivém bodu, skrze který data putují, a bývá tak omezena rychlostí internetového připojení jednotlivých uživatelů.

Do sítě TOR lze přistupovat několika způsoby. Prostřednictvím samostatného softwaru (který také umožňuje stát se routerem), speciálně upraveného prohlížeče (např. OperaTor, XB Browser od Mozilly, TorBrowser) či díky doplňku nainstalovaného do stávajícího prohlížeče (např. FoxTor).

JonDonym

JAP (Java AnOn Proxy) nazývaná též JonDonym je javová aplikace vytvářená jako společný projekt Technické univerzity v Drážďanech a Univerzity v Regensburgu. Pracuje na velmi podobném principu jako anonymizační síť TOR, jen místo jednotlivých routerů využívá tzv. Mix serverů[85]. Prvním krokem je inicializace celé komunikace skrze program JonDonym, který prostřednictvím vlastního proxy serveru změní IP adresu uživatelova počítače, data zašifruje a odešle do jednotlivých Mixů, vybraných uživatelem. V Mixech se pohybují data všech aktuálních uživatelů pod stejnou IP adresou prvního proxy serveru, čímž znemožňují identifikovat uživatele. Poslední mix server pak přidělí jednotlivým datům novou IP adresu a odešle požadavek na cílový server. Jednotlivé Mix servery jsou provozovány vybranými nezávislými institucemi a uživatel si může vybrat trasu datového toku podle poskytovatelů, kterým věří.

Využít služeb anonymizéru JonDonym je možné prostřednictvím volně dostupného softwaru, který je třeba doplnit o speciálně upravený vyhledávač JonDoFox, který je modifikovanou verzí prohlížeče Firefox.

[85] Servery ověřených poskytovatelů, které slouží k přenosu dat. Všechna procházející data jsou kvůli zvýšení bezpečnosti „smíchána“ dohromady - odtud název Mix servery.

4.3. Odstranění digitálních stop

Pokud se uživateli podaří zjistit rozsah své digitální stopy a určit subjekty, které mohou jeho data ukládat, přichází na řadu těžší část – tyto stopy odstranit. Hned na začátek je potřeba říci, že smazat všechny digitální stopy je v dnešní době prakticky nemožné, jak dokazuje CEO firmy Reputation Defender zabývající se správou online identity Michael Fertik. I přesto, že se v Reputation Defender věnují mazání digitálních stop na profesionální úrovni a uzavírají dohody s mnoha subjekty uchovávajícími osobní informace a data uživatelů, jako například Direct Marketing Association či people search enginy Spokeo, WhitePages, PeopleFinders apod., dokáží smazat „pouze“ 80-90 % dostupných osobních informací[86].

Zdánlivě nejjednodušší možnosti odstranění stop nabízejí zdroje spravované samotným uživatelem, u kterých má určitou kontrolu nad svými daty. U vlastních webových stránek či osobního blogu je zveřejňovaný obsah plně v režii uživatele a zajistit tak jeho nezávadnost je velmi snadné. Problém však nastává v případě webových služeb a sociálních sítí, kde již kontrola nad sdílenými daty není zdaleka tak velká, jak si většina uživatelů myslí. Tyto služby totiž vyžadují při registraci odsouhlasení licenčních podmínek, které obvykle obsahují povolení k využívání nahraného obsahu. Zde představím tři ukázky takového povolení:

Facebook

„…udělujete nám nevýhradní, přenosnou, převoditelnou, celosvětovou bezúplatnou (royalty-free) licenci na použití veškerého obsahu podléhajícího DV, který zveřejníte na Facebooku nebo v návaznosti na něj.“[87]

Google

„Pokud nahrajete nebo jinak odešlete obsah do našich služeb, poskytujete společnosti Google (a subjektům, se kterými společnost Google spolupracuje) celosvětově platnou licenci k užití, hostování, uchovávání, reprodukování, upravení, vytvoření odvozených děl (například děl, jež jsou výsledkem překladu, přizpůsobení/adaptací či úprav provedených za účelem jeho lepšího fungování v rámci

[86] MARTÍNEZ-CABRERA, ref. 75.

[87] Prohlášení o právech a povinnostech. FACEBOOK. *Facebook* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.facebook.com/legal/terms

našich služeb), komunikaci, publikování, provozování a zobrazování na veřejnosti a distribuci takového obsahu.“[88]

Yahoo!

„Pro fotografie, grafické prvky, zvuk a video, které odesíláte nebo zpřístupňujete na veřejně přístupných místech Služeb Yahoo! udělujete společnosti Yahoo! celosvětovou, bezplatnou a nevýhradní licenci k používání, distribuci, reprodukci, adaptaci, zveřejňování, překladu, vytváření odvozených děl, veřejnému předvádění a veřejnému zobrazování uživatelského obsahu ve Službách Yahoo! ... Pro veškerý ostatní uživatelský obsah, který odešlete nebo zpřístupníte pro zahrnutí na veřejně přístupných místech Služeb Yahoo!, udělujete celosvětovou, bezplatnou, nevýhradní, trvalou, neodvolatelnou licenci, ke které lze v plném rozsahu poskytovat sublicence, k používání, distribuci, reprodukci, adaptaci, zveřejňování, překladu, vytváření odvozených děl, veřejnému předvádění a veřejnému zobrazování uživatelského obsahu kdekoli v síti Yahoo! “[89]

Některé služby (Google, Yahoo!) si toto právo ponechávají i po smazání obsahu uživatelem, jiným (Facebook, Twitter) smazáním toto právo zaniká. Jak jsem však již ukázal v kapitole 4.1.2, smazáním informací na sociální síti Facebook se tyto informace stanou pouze nedostupnými pro uživatele, ale jejich kopie zůstávají dále uloženy na serveru provozovatele a existuje tedy možnost, že v budoucnu opět někde objeví (například po úspěšném hackerském útoku). I pouhým znepřístupněním obsahu pro veřejnost však lze ve většině případů předejít mnohým hrozbám jejich zneužití.

Pokud se uživatel rozhodne pro zrušení celého účtu u některé z webových služeb, může setkat s nečekaným odporem. Jelikož je vysoký počet uživatelů základním předpokladem jejich úspěchu (a tím pádem i zisků), snaží se uživatelům odchod co nejvíce ztížit. Proces a všechny nástrahy rušení účtu u 14 oblíbených služeb, včetně hodnocení jejich obtížnosti, popsala Cameron Chapman v článku pro Smashing

---

[88] Smluvní podmínky společnosti Google. GOOGLE. *Google*: *zásady a pravidla* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.google.com/intl/cs/policies/terms/regional.htm

[89] Podmínky poskytování služeb. YAHOO!. *Yahoo! Info Center* [online]. 2012 [cit. 2012-07-30]. Dostupné z: http://info.yahoo.com/legal/cz/yahoo/utos/terms/

magazine[90]. Na stupnici od 1 do 5 dopadl nejhůře z testovaných Facebook (5), následovaný serverem MySpace (4), LinkdeIn, Google, Ebry, Youtube (3). Pouze pět služeb nabízelo možnost lehkého odstranění účtu – Twitter, Flickr, Windows live (2) a StumbleUpon a PayPal (1). Samostatnou kategorii pak tvoří blogovací server WordPress a otevřená encyklopedie Wikipedia, které zrušení účtu neumožňují vůbec[91]. V takovém případě Cameron Chapman doporučuje smazání veškerého obsahu a změnu všech povinných osobních informací v účtu, aby již nebylo možné jej dále nijak spojit s původním uživatelem.

Alespoň částečně automatizovanou eliminaci aktivních stop nabízí nástroj Web 2.0 Suicidal Machine[92], který dokáže pomocí skriptu automaticky odstranit veškeré informace z vybraných sociálních sítí. Ke svému fungování však potřebuje získat přihlašovací údaje a tím plný přístup k těmto účtům. Právě díky nutnosti odevzdání přístupových údajů tento nástroj sítě Facebook a Linked In blokují. Aktuálně je tedy dostupný pouze pro sítě MySpace a Twitter. Je také potřeba říci, že zpřístupnění účtu plného osobních informací jak uživatele, tak všech jeho přátel, představuje určité bezpečnostní riziko, které někteří uživatelé nemusí být ochotni přijmout.

V případě, že jsou nechtěné informace umístěny na cizích webových stránkách, u kterých není správa obsahu v rukou uživatele, je potřeba kontaktovat správce dané stránky. Jedná-li se o osobní údaje zveřejněné v rozporu se zákonem 101/2000 Sb. o ochraně osobních údajů[93], může uživatel požadovat jejich vymazání na základě § 21. Stejný postup pak může uplatnit ve všech zemích Evropské unie, jelikož zákon 101/2000 Sb. přímo vychází z již zmíněné závazné evropské legislativy 95/46/ES. Jelikož je však internet prostorem „bez hranic“ může nastat situace, kdy jsou osobní údaje zveřejněny na zahraničním serveru subjektem, který nepodléhá evropským zákonům (například v Evropě nepodniká). V takovém případě podléhá zákonům dané země, na jejímž území se nachází, což může představovat vzhledem různě nastaveným

[90] CHAPMAN, Cameron. *Smashing magazine* [online]. June 11th, 2010 [cit. 2012-07-30]. Dostupné z: http://www.smashingmagazine.com/2010/06/11/how-to-permanently-delete-your-account-on-popular-websites/

[91] U Wikipedie se jedná o celkem pochopitelný krok. Vzhledem k její otevřené povaze je potřeba, aby byly všechny příspěvky spojeny s jasným autorem, popřípadě více autory.

[92] http://suicidemachine.org/

[93] Česko. ZÁKON ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000. Dostupné z: http://www.uoou.cz/files/101_cz

podmínkám ochrany osobních údajů problém. Správci webových stránek tak takovýmto žádostem nemusí vyhovět, pokud jim to neukládá zákon.

U pasivních digitálních stop, tedy zejména zájmových profilů u reklamních společností, záleží doba jejich uchovávání, možnosti kontroly a odstranění na přístupu jednotlivých subjektů. Na příkladu pěti společností, které podle serveru knowyourelements.com[94] patří mezi deset největších společností zabývajících se celosvětově sledováním uživatelů, předvedu, jak odlišný tento přístup může být.

> ***Lotame*** uchovává data po dobu 9 měsíců od jejich získání a neumožňuje uživatelům žádnou kontrolu ani manipulaci s těmito daty[95].
>
> ***Media Mind*** také neposkytuje možnost ovlivňovat získaná data ze strany a data uchovává po dobu 13 měsíců[96].
>
> ***Exulante*** vychází uživatelům nejméně vstříc, jelikož neposkytuje žádné informace o době ukládání získaných informací ani o tom, zda je mohou uživatelé nějakým způsobem získat či upravit[97].
>
> ***BlueKai*** na rozdíl od předcházejících společností umožňuje prostřednictvím aplikace BlueKai Registry[98] nahlížet a do jisté míry upravovat a odstraňovat nežádoucí informace přiřazené k danému počítači. Pokud uživatel nepřistoupí k vlastní úpravě, ponechává si data 6 měsíců[99].
>
> ***Omniture*** stejně jako u BlueKai mohou uživatelé zjistit a částečně spravovat informace obsažené v profilu. Získaná data však drží, dokud potřebuje, nestanovuje žádnou dobu, po které by automaticky docházelo k jejich odstranění[100].

Pokud tedy tyto společnosti kontrolu dat neumožňují, ale mají nastavenou dobu jejich expirace, mohou uživatelé přistoupit k jejich eliminaci tak, že využijí dostupné

---

94 EVIDON, Inc. *Know Your Elements* [online]. c2011 [cit. 2012-05-14]. Dostupné z: http://www.knowyourelements.com/

95 Lotame Privacy Policy. *Lotame* [online]. November 2, 2011 [cit. 2012-07-30]. Dostupné z: http://lotame.com/legal

96 Privacy Policy. *MediaMind* [online]. May 5, 2011 [cit. 2012-07-30]. Dostupné z: http://www.mediamind.com/privacy-policy

97 Website privacy policy. *EXlate* [online]. October 2010 [cit. 2012-07-30]. Dostupné z: http://exelate.com/consumer-opt-out/website-privacy-policy/

98 BlueKai Registry. *BlueKai* [online]. 2012 [cit. 2012-07-30]. Dostupné z: http://www.bluekai.com/registry/

99 Privacy Policy. *BlueKai*: *About Us* [online]. March 21, 2012 [cit. 2012-07-30]. Dostupné z: http://www.bluekai.com/privacypolicy.php

100 Privacy Policy. *Omniture*: *Privacy Center* [online]. May 7, 2012 [cit. 2012-07-30]. Dostupné z: http://www.omniture.com/en/privacy/policy

metody (opt-out, správa cookies a softwarové řešení) aby účinně zamezili dalšímu sběru dat, a pak vyčkat, dokud již získaná data nebudou po uplynutí stanovené doby smazána.

5. Porovnání volně dostupných nástrojů pro ochranu soukromí

Vzhledem k velkému počtu různých způsobů, jakými lze prostřednictvím internetu narušit něčí soukromí, vzniká také velké množství nástrojů, kterými si lze soukromí před těmito hrozbami chránit. Ty se liší například typem (samostatně stojící software či plugin), účinností, dostupností na jednotlivých platformách, ale zejména svými funkcemi, jelikož obvykle chrání pouze před určitým typem zneužití. Proto je potřeba před samotným porovnáním vyčlenit skupiny, v jejichž rámci se dále budou vybrané nástroje porovnávat. Skupiny jsou zvoleny záměrně tak, aby pokrývaly celou problematiku pasivních digitálních stop a jejich kombinací bylo možné dosáhnout co nejlepší možné ochrany. Kritériem pro výběr nástrojů je pak u všech skupin počet stažení na tematických webových serverech. Vzhledem k rozdílným povahám jednotlivých nástrojů budou přesnější kritéria stanovena až v rámci samotných skupin.

1. Nástroje zabraňující sledování aktivit
2. Nástroje zajišťující anonymitu v prostředí internetu
3. Nástroje pro odstranění uložených sledovacích zařízení

5.1. Nástroje zabraňující sledování aktivit

Pokud mají uživatelé obavu o své soukromí, nejjednodušším způsobem, jak mohou zamezit monitorování svých aktivit je použití pluginů, tedy doplňků běžně dostupných prohlížečů. Na rozdíl od samostatně stojících nástrojů, které budou předmětem porovnání v další kapitole, nevyžadují po uživatelích pro své správné nastavení a fungování žádné širší znalosti. Vzhledem ke své jednoduchosti a minimálním požadavkům se tak mohou stát nástroji pro ochranu soukromí využívanými širokou veřejností.

Podle aktuálních statistik[101] patří mezi tři nejoblíbenější prohlížeče v celosvětovém měřítku Internet Explorer, Google Chrome a Mozilla Firefox. Jelikož prohlížeč Internet Explorer nezobrazuje u jednotlivých doplňků počty stažení, volba prohlížeče pro sestavení žebříčku stahovanosti se zúžila pouze na Chrome a Firefox. Vzhledem k relativní mladosti prohlížeče Chrome byl nakonec zvolen Firefox, který

[101] Global Web Stats: June 2012. *W3Counter* [online]. June 2012 [cit. 2012-07-30]. Dostupné z: http://www.w3counter.com/globalstats.php?year=2012&month=6

zkoumané doplňky nabízí po delší dobu a jeho statistiky tak poskytují větší vypovídací hodnotu. Jedná se tedy o čtyři nejstahovanější pluginy na ochranu před sledováním internetových aktivit v prohlížeči Firefox[102] (pro lepší komparaci jsou uvedeny i počty stažení pro Chrome[103]): Ghostery (Firefox 631 971 – Chrome 359 989), TrackMeNot (Firefox 39 535 – Chrome 4 272), Do not track + (Firefox 157 675 – Chrome 153 905), TrackerBlock (Firefox 47 587 – Chrome 10 385). Přestože mají vybrané nástroje stejný cíl, dosahují ho různými způsoby. Sledovanými kritérii tedy budou u těchto nástrojů způsoby, jakými dokáží ochránit své uživatele před různými typy hrozeb.

5.1.1. TrackerBlock

TrackerBlock (verze 2.2) je nástroj od známé organizace Privacy Choice zabývající se ochranou soukromí na internetu. Je dostupný pro prohlížeče Firefox, Internet Explorer 9 a v opt-out verzi (Keep MORE Opt Outs) také pro Google Chrome. Jeho základem je databáze více jak 580 společností, sledujících uživatele a jejich online aktivity. K zabránění sledování pak TrackerBlock používá čtyř různých prostředků:

1. ***Nastavení hlavičky <DNT>*** - která informuje společnosti, že si uživatel nepřeje být sledován.
2. ***Ochrana cookies*** – umožňuje zablokovat ukládání, přepisování, ale i čtení již uložených souborů cookies.
3. ***Opt-out cookies*** – u vybraných společností nastaví opt-out cookies pro vyvázání se z doručování cílené reklamy; u některých společností funguje také proti dalšímu sběru dat.
4. ***Ochrana HTML5*** – rozšiřující specifikace jazyka HTML5 umožnuje webovým stránkám ukládat data podobná souborům cookies, která pomáhají např. rychlejšímu načítání stránek při jejich opětovné návštěvě, firmy však tento postup zneužívají pro ukládání souborů pro sledování uživatelských návyků, na tyto soubory se nevztahuje běžné mazání

[102] Soukromí a bezpečnost. MOZILLA CORPORATION. *Doplňky a aplikace Firefox* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://addons.mozilla.org/cs/firefox/extensions/privacy-security/?sort=users

[103] GOOGLE. *Internetový obchod Chrome* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://chrome.google.com/webstore

browser cookies[104]. TrackerBlock dokáže zjistit, zda jsou tato dat ukládána a zajistí jejich smazání.

I přes relativně vysoký počet a rozmanitost prostředků, kterými TrackerBlock chrání soukromí, se jedná spíše o ochranu pasivní (respektování DNT a opt-outs záleží na vůli třetí strany) a stále existuje množství jiných zařízení, kterými lze i přes jeho použití sledování realizovat (JavaScrip, pixelové tagy apod.). Výhodou oproti ostatním nástrojům je ochrana před relativně novým druhem sledování prostřednictvím HTML5, kterou zatím jiné nástroje nenabízí. Také umožňuje nastavit automatické mazání flash objektů při ukončení relace.

Výhodou tohoto nástroje také je, že vše probíhá automaticky v pozadí a není třeba nastavovat omezení pro každou společnost zvlášť. V případě, že by uživatel z nějakého důvodu chtěl jakoukoliv možnost u vybrané společnosti povolit, lze tak velmi jednoduše učinit v nastavení.

5.1.2. Ghostery

Ghostery 2.8.0.2 je výtvorem firmy Evidon, která se prezentuje jako nový typ společnosti, stojící mezi uživatelem, reklamními společnostmi a vládou. Doplněk Ghostery je dostupný pro všechny běžně využívané prohlížeče - Chrome, Internet Explorer, Firefox, Opera a Safari. Jeho databáze obsahuje více jak 1 000 různých subjektů a je pravidelně aktualizována. Jelikož by společnost měla sloužit jako prostředník mezi uživatelem a reklamními společnostmi, neblokuje Ghostery nalezená zařízení primárně, ale umožňuje uživateli získat informace o dané společnosti a na jejich základě rozhodnou, zda vybraná sledovací zařízení zablokovat, či nikoliv.

Ghostery funguje na principu detekce neviditelných sledovacích zařízení na navštívené webové stránce a následného zablokování jejich zdrojového kódu. Dokáže odhalit a zablokovat následující zařízení:

[104] MEDIATI, Nick. Lawsuit: Ad Network Could Be Tracking You With HTML5. In: *PCWorld*: *GeegTech* [online]. Sep 21, 2010 [cit. 2012-07-30]. Dostupné z: https://www.pcworld.com/article/205950/lawsuit_ad_network_could_be_tracking_you_with_html5.html

1. ***Obrazové objekty*** – například pixelové tagy
2. ***Iframes*** **-** tag <iframe> umožňuje vložit na stránky rám, ve kterém je zobrazena jiná, tzv**.** vnořená webová stránka.
3. ***Vložené objekty a tagy*** **-** například vložené pluginy sociálních sítí
4. ***Kontroluje a zabraňuje nechtěnému přesměrování***
5. ***Dynamicky vkládané elementy*** **–** například objekty vkládané skrze JavaScrip
6. ***Cookies*** **–** umožňuje blokovat ukládání cookies vybraných společností

Na rozdíl od předchozího nástroje TrackerBlock funguje jako aktivní ochrana a blokováním účinně zabraňuje sledování mnoha obvykle používanými nástroji, jako jsou web bugy, pixelové tagy, cookies, e-tagy či javové objekty. Vzhledem k blokování jejich zdrojového kódu může dojít na určitých webových stránkách k omezení jejich funkčnosti. V takovém případě je možné prostřednictvím whitelistu povolit určitý prvek na dané stránce, aniž by došlo k jeho odblokování i na všech ostatních, čímž lze dosáhnout lepšího kompromisu mezi funkčností a ochranou soukromí. Stejně jako TrackerBlock dovoluje automatické mazání flash a Silverlight cookies po ukončení prohlížení.

5.1.3. Do Not Track+

Nástroj Do Not Track+ verze 2.2.1.611 od firmy Abine pracuje na základě databáze čítající více jak 600 subjektů a je dostupný pro prohlížeče Chrome, Internet Explorer, Firefox a Safari. Kromě drobných odlišností je jeho funkčnost totožná s nástrojem Ghostery. Slouží tedy k detekci a zablokování skrytých sledovacích zařízení. Na rozdíl od Ghostery však Do Not Track+ nedokáže mazat soubory cookies, přidává však ke komunikaci navíc hlavičku DNT. Nalezená sledovací zařízení také blokuje primárně, s možností jejich zpětného povolení.

Ghostery vs. Do Not Track+

Vhledem k totožnému účelu, jsem se rozhodl ověřit jejich funkčnost přímým srovnáním počtu nalezených sledovacích zařízení na vybraných stránkách. Jedná se o deset vybraných českých serverů, které patří mezi pětadvacet

nejnavštěvovanějších[105], dále pět celosvětově nejnavštěvovanějších webů[106] a tři, které podle mých dřívějších zkušeností obsahují velký počet těchto zařízení. Nástroje byly testovány odděleně, aby nedocházelo k vzájemnému ovlivňování výsledků[107].

Doména (pořadí v návštěvnosti)	**GHOSTERY**	**DNT+**	**Počet rozdílných zařízení**
seznam.cz (1)	1	0	1
idnes.cz (2)	3	3	4 (2+2)
centrum.cz (3)	4	2	2 (2+0)
lide.cz (4)	1	0	1
stream.cz (6)	0	0	0
aukro.cz (8)	4	2	4 (3+1)
estranky.cz (15)	4	3	3 (2+1)
invia.cz (13)	3	1	2 (2+0)
blog.cz (19)	4	4	0
csfd.cz (23)	3	1	2 (2+0)
Google	0	0	0
Facebook	0	0	0
Yahoo!	1	2	2 (0+1)
Youtube	1	2	1 (0+1)
MSN (6)	4	8	4 (0+4)
Dictionary	7	9	4 (2+2)
Mashable	13	13	4 (2 + 2)
Wall Street Journal	8	14	8 (1+7)
Celkový počet nalezených zařízení	61	64	
Vyšší počet nalezených zařízení	7	5	

Tabulka 1 - Porovnání nástrojů Ghostery a Do Not Track+

[105] Weby byly vybírány s ohledem na tematickou rozmanitost.
TOP weby českého internetu: Průběžně aktualizovaný žebříček TOP českých webů, podle hodnocení serveru Siteinfo. *Siteinfo* [online]. 2012 [cit. 2012-07-30]. Dostupné z: http://www.siteinfo.cz/top-weby

[106] Web Wikipedia byl záměrně vynechán, jelikož je známo, že žádná zařízení neobsahuje a pro účely porovnání tak nemá význam jej začleňovat.
Top 15 Most Popular Websites: July 2012. *EBizMBA*: *The eBusiness Knowledgebase* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.ebizmba.com/articles/most-popular-websites

[107] Při souběžném provozu Do Not Track+ nezaznamená nástroje, které jsou již deaktivovány pomocí Ghostery, čímž také dokazuje jeho funkčnost.

Ghostery nalezlo vyšší počet sledovacích zařízení celkem v sedmi případech, Do Not Track+ pak pouze v pěti případech. V dalších šesti případech došlo ke shodě. I přesto v celkovém součtu našel nástroj Do Not Track o tři sledovací zařízení více, tedy 64.

Rozdíly však nevznikaly pouze v počtech, ale zejména v typech nalezených zařízení, které se odvíjí od používané databáze. Jak lze vidět například u portálu iDnes, oba nástroje nalezly shodně po třech zařízeních a přesto se ve čtyřech případech jednalo o nástroj, který konkurent nezaznamenal. Tyto rozpory pak vznikaly i u dalších testovaných webů. Ghostery a Do Not Track+ se vzájemně doplňují, a jelikož mohou bez problému pracovat současně, je jejich kombinace ideální pro maximalizaci zabezpečení před sledováním třetími stranami.

5.1.4. TrackMeNot

TrackMeNot (testována aktuální verze 0.6.728) vznikl jako projekt na New York University. Jeho účelem je zabránit kontrolování a následnému profilování uživatelů na základě dotazů zadávaných do vyhledávačů. Princip je velmi jednoduchý – TrackMeNot zasílá v nastavených intervalech smyšlené (ale smysluplné) dotazy různých oborů do vybraných vyhledávačů. Tyto dotazy, uložené spolu s pravými dotazy od uživatele v historii hledání, zkreslují obraz uživatelových zájmů a do jisté míry tak znemožňují jejich odhalení a složení zájmového profilu. Dostupný je pro prohlížeče Firefox a Chrome.

Aby bylo tyto falešné dotazy co nejsložitější odfiltrovat, nabízí TrackMeNot množství nastavení a užitečných funkcí. Základem je výběr vyhledávače, který zajistí zasílání dotazů pouze do vyhledávače, který uživatel využívá a zabrání tak vzniku dalších (i když falešných) profilů spojených s jeho IP adresou. TrackMeNot je schopný zasílat dotazy do vyhledávačů AOL, Yahoo!, Google a Bing. Druhým předpokladem pro správnou funkci je nastavení zdroje pro dotazy. Standardě je jako zdroj nastaven RSS kanál deníku NY Times a další americké zpravodajské servery, ze kterého získává aktuální témata pro tvorbu dotazů, které však nejsou vhodné pro všechny uživatele. Proto TrackMeNot umožňuje nastavit libovolný RRS kanál či sadu dotazů, které budou více odpovídat (například jazykově) uživatelovým běžným hledáním. Nejnovější verze

také, pro větší věrohodnost, simuluje údery do klávesnice, otevírání odkazů ve výsledcích vyhledávání či automaticky vybírá místo zadávání (hlavní stránka, lišta apod.) podle uživatelových zvyklostí a snaží se tak maximálně přizpůsobit podobu běžnému vyhledávání.

I přesto, že je TrackMeNot velmi úzce zaměřen, jedná se o velmi užitečný nástroj, jelikož poskytuje typ ochrany, který nenabízí žádný jiný nástroj.

5.1.5. Konečná komparace

	Ghostery	DNT +	TrackerBlock	TrackMeNot
cookies	✓	✓	✓	✗
pixelové tagy	✓	✓	✗	✗
web bug	✓	✓	✗	✗
Flash	✓	✓	✗	✗
vložené objekty (pluginy)	✓	✓	✗	✗
HTML5	✗	✗	✓	✗
opt-out	✗	✓	✓	✗
hlavička DNT	✗	✓	✓	✗
vyhledávání	✗	✗	✗	✓
Java	✓	✓	✗	✗
Celkem	50%	70%	40%	10%

Tabulka 2 - Celkové porovnání vybraných nástrojů zabraňujících sledování aktivit

V celkovém porovnání dopadl nejlépe nástroj Do Not Track+, který dokáže zabránit před sledováním celkem sedmi různými typy sledování. Oproti konkurenci (TrackerBlock a TrackMeNot) nabízí zejména aktivní ochranu proti skrytým sledovacím zařízením, jako jsou web bugy či pluginy sociálních sítí. Oproti přímému konkurentovi Ghostery, kterého předčil i v dílčím testu, pak přidává ještě nastavení hlavičky DNT a opt-out cookies. Do Not Track+ tak vychází jako nejlepší nástroj pro ochranu před sledováním aktivit v prostředí internetu. Druhý skončil nástroj Ghostery, jehož výhodou je zejména aktivní ochrana před skrytými prvky.

TrackerBlock sice nedokáže ochránit před pixelovými tagy ani jinými neviditelnými zařízeními, poskytuje však ochranu před novým typem HTML5. Poslední se umístil nástroj TrackMeNot, který díky svému specifickému zaměření chrání pouze před jedním typem sledování, ovšem takovým, které jiné nástroje nenabízí.

Ačkoliv se testované nástroje v mnoha funkcích shodují, vždy přináší oproti konkurenci něco navíc. Optimální úrovně ochrany tak lze dosáhnout až jejich kombinací.

5.2. Nástroje zajišťující anonymitu v prostředí internetu

Dalším způsobem, jak chránit své soukromí před nechtěným sledováním, je použití anonymizačních nástrojů. Jak vyplývá z kapitoly 4.2.5. volně dostupných možností, jak skrýt svou identitu není mnoho. Objekty porovnání zde budou nástroje TOR a JonDonym, které patří na portálu Softpedia[108] mezi nejstahovanější (JonDonym 177 988 stažení – TOR 65 870 stažení) nástroje pro anonymní pohyb po internetu a pro lepší porovnání variability možností také webový proxy server The Cloak, nabízející velké množství nastavení[109]. Anonymní módy prohlížečů do porovnání nezahrnuji, jelikož ve skutečnosti nenabízí prakticky žádnou formu anonymity, pouze neukládají webovou historii.

Cílem komparace je zjistit jak velkou míru anonymity nabízejí jednotlivé nástroje a kolik potencionálně identifikujících informací je možné i přes jejich použití získat. Pro tento účel jsem použil online test anonymity IP-check[110] vytvořený Technickou univerzitou v Drážďanech a Univerzitou v Regensburgu, který nabízí komplexní testování velkého množství běžně sledovaných informací a kvalitní grafický výstup.

5.2.1. Běžně využívané prohlížeče

Aby bylo možné porovnat, jak velké zlepšení v ochraně soukromí jednotlivé nástroje nabízí, je potřeba nejdříve nastínit, kolik informací je možné běžně zjistit

[108] Downloads tagged with: anonimity. *Softpedia* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.softpedia.com/downloadTag/anonimity

[109] *The Cloak*: *free anonymous web surfing* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.the-cloak.com/

[110] IP Check. *JonDonym*: *the anonymisation service* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://ip-check.info/?lang=en

při použití standardního prohlížeče. Základem pro porovnání tedy budou výsledky stejného testu tří nejvyužívanějších – Internet Explorer, Firefox, Chrome.

Internet Explorer 9

Your IP	217.30.64.34	Traceroute
Your location	Hlavni mesto Praha, Prague	Show on map
Your net provider	Planet A,a.s.	Whois IP
Reverse DNS	gw-cmo.aim-net.cz	Whois Domain

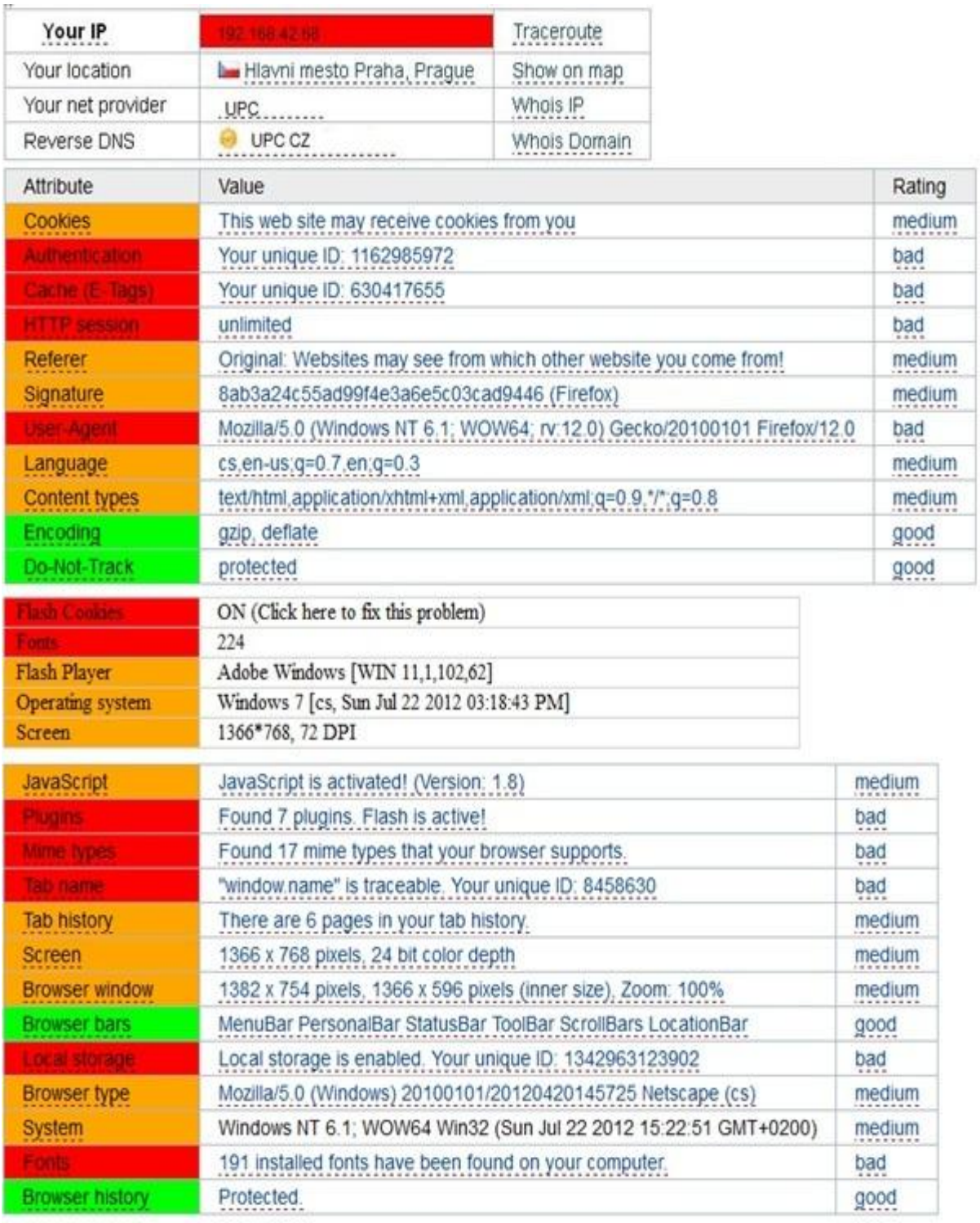
Attribute	Value	Rating
Cookies	Third party sites get your cookies and may track you.	bad
Authentication	Your unique ID: 804788603	bad
Cache (E-Tags)	Your unique ID: 1101427220	bad
HTTP session	unlimited	bad
Referer	Original: Websites may see from which other website you come from!	medium
Signature	84f83c14f83b5f89c8c963672fe84057 (Internet Explorer)	medium
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	bad
Language	cs-CZ	medium
Content types	text/html, application/xhtml+xml, */*	medium
Encoding	gzip, deflate	good
Do-Not-Track		medium

Flash Cookies	ON (Click here to fix this problem)
Fonts	224
Flash Player	Adobe Windows [WIN 10,3,181,34]
Operating system	Windows 7 [cs, Sat Jul 28 2012 09:43:36 AM]
Screen	1366*768, 72 DPI

JavaScript	JavaScript is activated! (Version: 1.3)	medium
Plugins	Found 3 plugins. Flash is active! Your unique ID: {3300AD50-2C39-46c0-AE0A-000000000000}	bad
Tab name	"window.name" is traceable. Your unique ID: 5788551	bad
Tab history	There are 5 pages in your tab history.	medium
Screen	1366 x 768 pixels, 24 bit color depth	medium
Browser window	1382 x 754 pixels, 1366 x 651 pixels (inner size), Zoom: 100%	medium
Local storage	Local storage is enabled. Your unique ID: 1343461415935	bad
Browser type	Microsoft Internet Explorer (cs)	medium
System	Win32 x86 (cs, windows-1250, Sat Jul 28 09:47:39 UTC+0200 2012)	medium
Fonts	Do you see strange symbols here? If yes, your fonts are readable!	good
Browser history	Protected.	good

Obrázek 1 - Výsledky testu anonymity Internet Explorer

Mozilla Firefox 14.0.1



Your IP	[redacted]	Traceroute
Your location	Hlavni mesto Praha, Prague	Show on map
Your net provider	UPC	Whois IP
Reverse DNS	UPC CZ	Whois Domain

Attribute	Value	Rating
Cookies	This web site may receive cookies from you	medium
Authentication	Your unique ID: 1162985972	bad
Cache (E-Tags)	Your unique ID: 630417655	bad
HTTP session	unlimited	bad
Referer	Original: Websites may see from which other website you come from!	medium
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	medium
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0	bad
Language	cs,en-us;q=0.7,en;q=0.3	medium
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	medium
Encoding	gzip, deflate	good
Do-Not-Track	protected	good

Flash Cookies	ON (Click here to fix this problem)
Fonts	224
Flash Player	Adobe Windows [WIN 11,1,102,62]
Operating system	Windows 7 [cs, Sun Jul 22 2012 03:18:43 PM]
Screen	1366*768, 72 DPI

JavaScript	JavaScript is activated! (Version: 1.8)	medium
Plugins	Found 7 plugins. Flash is active!	bad
Mime types	Found 17 mime types that your browser supports.	bad
Tab name	"window.name" is traceable. Your unique ID: 8458630	bad
Tab history	There are 6 pages in your tab history.	medium
Screen	1366 x 768 pixels, 24 bit color depth	medium
Browser window	1382 x 754 pixels, 1366 x 596 pixels (inner size), Zoom: 100%	medium
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
Local storage	Local storage is enabled. Your unique ID: 1342963123902	bad
Browser type	Mozilla/5.0 (Windows) 20100101/20120420145725 Netscape (cs)	medium
System	Windows NT 6.1; WOW64 Win32 (Sun Jul 22 2012 15:22:51 GMT+0200)	medium
Fonts	191 installed fonts have been found on your computer.	bad
Browser history	Protected.	good

Obrázek 2 - Výsledky testu anonymity Mozilla Firefox

Google Chrome 20.0

Your IP	217.30.64.34	Traceroute
Your location	Hlavni mesto Praha, Prague	Show on map
Your net provider	Planet A,a.s.	Whois IP
Reverse DNS	gw-crno.aim-net.cz	Whois Domain

Attribute	Value	Rating
Cookies	This web site may receive cookies from you	medium
Authentication	Your unique ID: 1299225626	bad
Cache (E-Tags)	Your unique ID: 606383756	bad
HTTP session	unlimited	bad
Referer	Original: Websites may see from which other website you come from!	medium
Signature	2ca1c033ad7829d71da53b1e137b24ae (Chrome)	medium
User-Agent	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/536.11 (KHTML, like Gecko) Chrome/20.0.1132.57 Safari/536.11	bad
Language	cs-CZ,cs;q=0.8	medium
Charset	windows-1250,utf-8;q=0.7,*;q=0.3	medium
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	medium
Encoding	gzip,deflate,sdch	medium
Do-Not-Track		medium

Your internal IP	192.168.1.101 (Click here to fix this problem)
Java VM	Sun Microsystems Inc. 1.6.0_30
Operating system	Windows XP x86 Version 5.1
Language	Czech, Czech Republic

Flash Cookies	ON (Click here to fix this problem)
Fonts	234
Flash Player	Google Windows [WIN 11,3,300,265]
Operating system	Windows XP [cs, Sat Jul 28 2012 09:21:04 AM]
Screen	1280*800, 72 DPI

JavaScript	JavaScript is activated! (Version: 1.7)	medium
Plugins	Found 16 plugins. Java and Flash are active!	bad
Mime types	Found 118 mime types that your browser supports.	bad
Tab name	"window.name" is traceable. Your unique ID: 9333161	bad
Tab history	There are 4 pages in your tab history.	medium
Screen	1280 x 800 pixels, 32 bit color depth	medium
Browser window	1280 x 770 pixels, 1280 x 685 pixels (inner size)	medium
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
Local storage	Local storage is enabled. Your unique ID: 1343460050120	bad
Browser type	20030107 Netscape (cs)	medium
System	Win32 (windows-1250, Sat Jul 28 2012 09:25:48 GMT+0200 (Střední Evropa (letní čas)))	medium
Fonts	188 installed fonts have been found on your computer.	bad
Browser history	Protected.	good

Obrázek 3 - Výsledky testu anonymity Google Chrome

Jak vyplývá z výsledků testu, při surfování se všemi běžnými prohlížeči lze zjistit velké množství informací. Všechny prohlížeče poskytují v základním stavu pouze velmi malou ochranu soukromí; nejhůře dopadl prohlížeč Chrome, který dovoluje zjistit nejen IP adresu poskytovatele, ale i konkrétní IP adresu zařízení. Většina aktivit

je skrze tyto prohlížeče relativně snadno sledovatelná a to hned několika způsoby. Každá navštívená stránka získá informace o uživatelově IP adrese, poskytovateli připojení i jeho geografické lokalizaci[111]. Prostřednictvím ověřování (authentication) a e-tagů uložených v mezipaměti mohou třetí strany označit a sledovat uživatelovy aktivity stejně jako prostřednictvím souborů cookies. I přesto, že se tyto informace po zavření prohlížeče z jeho paměti vymažou, mohou představovat jisté riziko. HTTP session dovoluje poskytovateli připojení spojovat si jednotlivé uživatelovy požadavky a získat tak přehled o jeho zájmech a aktivitách. User agent poskytuje webovým stránkám informace o použitém operačním systému a spolu s javovými a flash aplikacemi také již zmíněný otisk prohlížeče a další informace. Další závažné problémy pro ochranu soukromí pak představují zejména povolené flash cookies a local storage, které mohou ukládat identifikační soubory do počítače a pluginy, prostřednictvím kterých je opět možné získávat informace o uživatelově činnosti, či hlavička „Referer“, odkazující na předchozí navštívenou webovou stránku. Vzhledem k faktu, že jsou výsledky jednotlivých prohlížečů prakticky totožné a jejich porovnání má pro práci pouze informativní charakter a slouží jen jako výchozí bod pro komparaci vybraných nástrojů, nebudou již tyto nástroje dále testovány na všech platformách. Pro lepší soudržnost jsem tedy zvolil prohlížeči Mozilla Firefox, který byl v rámci některých skupin již použit jako zdroj žebříčku pro jejich výběr.

[111] V obrázku 1 byly tyto údaje, kromě lokalizace, záměrně pozměněny a neshodují se tak se skutečným zařízením.

5.2.2. Webový anonymizér Cloak

Your IP	95.211.77.194 (Proxy) 192.168.42.68 [JavaScript]	Traceroute
Your location		Show on map

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E-Tags)	protected	good
HTTP session	unlimited	bad
Referer	Original: Websites may see from which other website you come from!	medium
Signature	047ffea3524c4b6e79f1ed5ad8e4f6d5 (Web-Proxy)	medium
User-Agent	Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101 Firefox/13.0.1	bad
Language		medium
Content types	*/*	medium
Encoding	deflate, gzip	medium
Do-Not-Track		medium

YOUR IP	192.168.42.68(Click here to fix this problem)
Flash Cookies	ON (Click here to fix this problem)
Fonts	234
Flash Player	Adobe Windows [WIN 11,3,300,265]
Operating system	Windows XP [cs, Sun Jul 22 2012 09:07:36 AM]
Screen	1280*800, 72 DPI

JavaScript	JavaScript is activated! (Version: 1.8)	medium
Plugins	Found 12 plugins.	bad
Mime types	Found 77 mime types that your browser supports.	bad
Tab name	"window.name" is traceable. Your unique ID: 9003332	bad
Tab history	There are 5 pages in your tab history.	medium
Screen	1280 x 800 pixels, 24 bit color depth	medium
Browser window	1288 x 778 pixels, 1280 x 620 pixels (inner size), Zoom: 100%	medium
Browser bars	MenuBar PersonalBar StatusBar ToolBar ScrollBars LocationBar	good
Local storage	Local storage is enabled. Your unique ID: 1342940854486	bad
Browser type	Mozilla/5.0 (Windows) 20100101/20120614114901 Netscape (cs)	medium
System	Windows NT 5.1 Win32 (Sun Jul 22 2012 09:08:43 GMT+0200)	medium
Fonts	200 installed fonts have been found on your computer.	bad
Browser history	Protected.	good

Obrázek 4 - výsledky testu při použití webového anonymizéru

Komunikace skrze webový proxy server oproti běžnému nezabezpečenému prohlížení zabraňuje pouze ukládání souborů pro ověřování, cookies, e-tagů do mezipaměti a neposkytuje informace o typu přenášeného obsahu a jazyku prohlížeče,

které jsou z hlediska ochrany soukromí méně důležité. Hlavním důvodem pro použití webových proxy serverů je obvykle skrytí vlastní IP adresy, které však v testu selhalo. Test zpočátku načte IP adresu daného proxy serveru, ovšem během několika vteřin je schopný pomocí speciálního Java scriptu odhalit IP adresu zařízení, ze kterého dotaz původně vzešel. Tento postup sice mnoho běžných webových stránek používat nemusí, nicméně takto obejít použitý proxy server není nemožné a jeho anonymizační schopnosti jsou tak silně limitovány. Celkově tedy webové anonymizéry nenabízí žádná zásadní vylepšení ochrany soukromí v porovnání s běžnými prohlížeči.

5.2.3. TOR

Your IP	93.182.129.86 (Tor)	Traceroute
Your location	Skane Lan, Lund	Show on map
Your net provider	Infra-trygg	Whois IP
Reverse DNS	exit3.ipredator.se	Whois Domain

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E-Tags)	Your unique ID: 397151197	bad
HTTP session	10 minutes (until your Tor identity is changed)	medium
Referer	Original: Websites may see from which other website you come from!	medium
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	good
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0	good
Language	en-us,en;q=0.5	good
Charset		medium
Content types	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	good
Encoding	gzip, deflate	good
Do-Not-Track	protected	good

JavaScript	JavaScript is currently turned off.	good
Browser window	1280 x 632 pixels (inner size)	medium
Fonts	Do you see strange symbols here? If yes, your fonts are readable!	good
Browser history		good

Obrázek 5 - výsledky testu při použití sítě TOR

Síť TOR testované verze *2.2.37-2* potřebuje, stejně jako JonDonym, ke svému fungování dvě části: klienta, který umožňuje přístup do sítě a různá nastavení a dále speciálně upravený prohlížeč (který vychází z klasického Firefoxu). Kromě toho,

že je komunikace realizována skrze kaskádu proxy serverů, čímž zaručuje ochranu identity, využívá také běžně dostupné a ověřené pluginy, které ještě více zvyšují bezpečnost. Jedná se o pluginy HTTPS Everywhere, který na všech webových stránkách, které to umožňují, vyžaduje zabezpečené připojení a NoScript, který zabraňuje fungování Flash a Java scriptů. Z tohoto důvodu také ve výsledcích testu chybí všechny položky, které je možné skrze tyto objekty zjistit. Ochrana soukromí je tedy na velmi dobré úrovni. Jediným slabým článkem je možnost ukládání e-tagů a zasílání HTTP hlaviček „Referer“, které poskytují informace o předchozí navštívení stránce. HTTP session se mění spolu s automatickou změnou identity, která probíhá každých deset minut. Měnit identitu však lze i ručně v libovolných časových intervalech, čímž lze zabránit sledování poskytovatelem připojení po dobu desetiminutového intervalu. Jazyk, typ prohlížeče a jeho podpis jsou stejné pro všechny uživatele sítě TOR a identifikace jednotlivce jejich prostřednictvím je tedy nemožná. Vyhledávání obsahu může být realizováno kromě standardních vyhledávačů také skrze vyhledávače DuckDuckGo a StartPage, které neukládají žádné záznamy o hledaných výrazech.

5.2.4. JonDonym

Your IP	212.117.177.5 (JonDonym)	Traceroute
Your location	Luxembourg	Show on map
Your net provider	root SA	Whois IP
Reverse DNS	anonymization-service.ya-trade.com	Whois Domain

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E-Tags)	protected	good
HTTP session	stateless	good
Referer	hidden (changed when switching the website)	good
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	good
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0	good
Language	en-us	good
Content types	text/html,application/xml,*/*	good
Encoding	gzip, deflate	good
Do-Not-Track	protected	good

JavaScript	JavaScript is currently turned off.	good
Browser window	1280 x 612 pixels (inner size)	medium
Fonts	Do you see strange symbols here? If yes, your fonts are readable!	good
Browser history		good

Obrázek 6 - výsledky testu při použití sítě JonDonym

Nejlepšího výsledku v testu anonymity dosáhla aplikace JonDonym[112] fungující se speciálně upraveným prohlížečem také na platformě Mozilla Firefox[113]. Verze JonDoFox je v základu vybavena čtyřmi bezpečnostními doplňky: NoScript, HTTPS Everywhere, Cookies monster pro správu různých druhů cookies a AdBlock+ pro blokování reklamních banerů (a tím i různých sledovacích zařízení, které skrze tyto banery fungují). Oproti aplikaci TOR tak navíc blokuje ukládání všech druhů sledovacích zařízení včetně e-tagů, HTTP session i hlaviček „Referer“. JonDonym sice nedokáže zfalšovat rozlišení obrazovky, nicméně tato informace sama o sobě

[112] Testovaná verze 00.18.001
[113] Testovaná verze 2.6.7

nepředstavuje vůbec žádné ohrožení soukromí. Samozřejmostí je pak také chráněné vyhledávání prostřednictvím vyhledávačů DuckDuckGo a StartPage.

5.2.5. Konečná komparace

	Cloak (web proxy)	TOR	JonDonym
IP adresa	✗	✓	✓
poskytovatel připojení	✓	✓	✓
geografická lokace	✓	✓	✓
otisk prohlížeče	✗	✓	✓
Java	✗	✓	✓
Flash	✗	✓	✓
historie	✓	✓	✓
cookies	✓	✓	✓
e-tags	✓	✗	✓
Referer	✗	✗	✓
Výsledek	50%	80%	100%

Tabulka 3 - porovnání anonymizačních nástrojů

Z výsledků porovnání je patrné, že míra ochrany soukromí velmi záleží na použitém anonymizačním prostředku. Z tohoto pohledu se webové proxy servery ukazují jako nevhodné, jelikož jejich funkčnost se nachází spíše na úrovni běžných anonymních módů prohlížečů, než plnohodnotných nástrojů. Přímými konkurenty jsou tak v tomto směru pouze kaskádové proxy sítě TOR a JonDonym. Oba nabízejí velmi vysokou úroveň anonymity a bezpečnosti, přesto však ze srovnání vychází lépe aplikace JonDonym, která ani dočasně neukládá informace o relaci do mezipaměti a neposkytuje informace o dříve navštívených stránkách prostřednictvím hlavičky „Referer“. V jeho prospěch mluví také fakt, že celá komunikace je vedena přes body ověřené certifikačními autoritami, na rozdíl od uzlů sítě TOR, které jsou počítači jednotlivých uživatelů, což může představovat jisté riziko. Společně s celkově lepším zázemím, možností založení dočasného e-mailu (např. pro účely jednorázové registrace)

či možností volby trasy a serverů, které zajistí uživatelovi krytí, je JonDonym ideálním nástrojem pro bezpečné a anonymní surfování.

5.3. Nástroje pro odstranění uložených sledovacích souborů

Jak bylo v průběhu práce již mnohokrát zmíněno, hlavní nástroj pro sledování aktivit stále představují identifikační soubory cookies, ukládané skrze prohlížeč do uživatelova zařízení. Pokud tedy uživatel nevyužívá nějaký nástroj (např. některý z výše porovnávaných) aby blokoval jejich ukládání, přepisování a čtení, je potřeba tyto soubory zpětně odstraňovat. Všechny běžně dostupné prohlížeče dnes nabízejí možnost mazání těchto souborů, a to buď ručně, či automaticky, například při ukončení prohlížeče. Tento postup však nemá žádný vliv na soubory cookies typu flash či Silverlight, ukládané multimediálními objekty. K automatickému odstraňování všech souborů umožňující identifikaci uživatele je tedy potřeba použít patřičné nástroje.

Pro porovnání jsem zde připravil tři nejstahovanější nástroje opět podle serveru Softpedia[114], které slouží i pro mazání těchto objektů a zároveň jsou dostupné zdarma: CCleaner (1,721 463 stažení), ATF Cleaner (183 034), Temp File Cleaner (31 852) a pro zlepšení porovnání již zmíněný doplněk Ghostery (který je i v rámci této funkce nejstahovanějším doplňkem). Kritériem pro testování je celkový počet druhů souborů, které dokáže nástroj odstranit a ochránit tak uživatele před sledováním.

5.3.1. CCleaner

Nástroj CCleaner ver. 3.21.1767 společnosti Piriform je jedním z nejoblíbenějších nástrojů pro optimalizaci chodu počítačových systému pomocí odstraňování nepotřebných souborů. Oblíbený je zejména díky své jednoduchosti, účinnosti, ale hlavně komplexnosti. Kromě nepotřebných systémových souborů, registrů, dočasných souborů apod. se tak dokáže plně postarat i o soubory spojené s internetovými prohlížeči Internet Explorer, Mozilla Firefox, Google Chrome, Opera a ve verzi pro systémy Mac také Safari. Z nich dokáže bezpečně odstranit dočasné soubory, historii prohlížení, historii stahování, vyplněné formuláře, hesla, ale hlavně všechny druhy cookies, včetně cookies typu flash a Silverlight. Uživatel má samozřejmě možnost vytvořit seznam chráněných cookies, na které se mazání nebude vztahovat.

[114] Download: Secure Cleaning. *Softpedia* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.softpedia.com/catList/98,0,1,0,1.html

Tímto krokem lze předejít odstranění cookies, které neslouží ke sledování aktivit, ale například pro zapamatování nastavení na určité webové stránce.

5.3.2. ATF Cleaner

Druhým nástrojem je ATF Cleaner 3.0.0.2 vytvořený organizací Atribune. Oproti předchozímu CCleaneru je více zaměřený na odstraňování souborů webových prohlížečů; správa souborů systémových je spíše doplňková a velmi omezená. ATF Cleaner si poradí se soubory cookies (s výjimkou flash a Silverlight), historií prohlížení a stahování, vyplněnými formuláři a hesly a informacemi uloženými v mezipaměti, a to u prohlížečů Internet Explorer, Mozilla Firefox a Opera. Vybrané položky maže vždy celé a nenabízí možnost tvorby whitelistu a ponechání souborů cookies pro vybrané subjekty, což může být pro některé uživatele velmi omezujícím prvkem.

5.3.3. Temp File Cleaner

Temp File Cleaner 4.0.2 je prostředek pro odstraňování dočasných souborů, který nabízí prakticky totožné funkce jako CCleaner. Kromě systémových souborů odstraňuje také informace uložené prostřednictvím internetových prohlížečů Internet Explorer, Mozilla Firefox, Opera, Google Chrome a multimediálních aplikací založených na Flash a Java. Ochranu soukromí poskytuje tedy před cookies, flash cookies, informacemi uloženými v mezipaměti, historii prohlížení a v historii stahování. Bohužel, stejně jako ostatní neumožňuje nastavení výjimek v rámci jednotlivých skupin mazaných souborů.

5.3.4. Ghostery

Ačkoliv je primárně Ghostery určené k aktivnímu blokování neviditelných sledovacích zařízení na webových stránkách, pro komplexnější ochranu nabízí také možnost automatického mazání flash a Silverlight cookies při ukončení prohlížení. Právě z tohoto důvodu jsem tento nástroj zařadil do porovnání i v rámci této kategorie. V tomto ohledu již však nenabízí žádné rozšířené nastavení ani možnost vytvoření výjimek.

5.3.5. Konečná komparace

	CCleaner	ATF Cleaner	Temp File Cleaner	Ghostery
cookies	✓	✓	✓	✗
flash cookies (LSO)	✓	✗	✓	✓
Silverlight cookies	✓	✗	✗	✓
cache (dočasné soubory)	✓	✓	✓	✗
historie prohlížení	✓	✓	✓	✗
Celkem	100%	60%	80%	40%

Tabulka 4 - porovnání nástrojů pro odstranění sledovacích souborů

Jako jediný z testovaných dokázal odstranit všechny soubory a informace, které jsou běžně využívány pro sledování online aktivit, program CCleaner. Přičtu-li jednoduchost ovládání, kompatibilitu s širokým spektrem platforem a zejména možnost nastavení seznamu výjimek, který jiné nástroje vytvořit neumí, vychází CCleaner z tohoto porovnání jako jasný vítěz. Druhý jak v počtu odstraněných položek, tak v celkovém pořadí skončil nástroj Temp File Cleaner, který jinak v mnoha ohledech konkuruje prvnímu CCleaneru. Mínusem ovšem je absence možnosti nastavení whitelistu a ochrany před únikem informací prostřednictvím Silverlight cookies. Ačkoliv se nástroj Ghostery v počtením srovnání umístil až za programem ATF Cleaner, v celkovém hodnocení vyhází lépe. Důvodem je fakt, že ATF Cleaner na rozdíl od Ghostery, které dokáže odstraňovat flash a Silverlight cookies, nabízí ochranu pouze před standardními soubory cookies, informacemi uloženými v mezipaměti a v historii prohlížení. Všechny tyto položky však zvládne stejně dobře odstranit jakýkoliv běžný prohlížeč i bez nutnosti dodatečných nástrojů. Z tohoto důvodu tak nemá využívání ATF Cleaneru vůbec žádný vliv na zvýšení ochrany soukromí.

6. Závěr

Díky měnící se podstatě osobních informací a internetového prostředí jako takového, je dnes téma digitálních stop velmi aktuální. A s největší pravděpodobností ještě dlouho zůstane. I přes to, že uživatelé stále vnímají soukromí ve světě fyzickém a digitálním odděleně, a nastavují tak pro ně rozdílná pravidla, již dávno tomu tak není a naše digitální identita je dnes stejně důležitá (a také zneužitelná) jako ta fyzická.

Cílem práce bylo zjistit, zda a do jaké míry může uživatel chránit své soukromí před narušením prostřednictvím informací získaných z jeho digitálních stop. Kontrola nad stopami aktivními je oproti stopám pasivním jednodušší, jelikož její vznik, správa a tudíž i výsledný rozsah závisí pouze na přístupu samotného uživatele. K ovlivnění počtu dostupných informací, fotografií, videí a jiných dat tvořících obraz jeho identity tedy není potřeba žádných speciálních nástrojů a chránit soukromí si uživatel může pouze jejich uvážlivým zveřejňováním. U stop pasivních je situace opačná. Nad jejich vznikem ani následnou správou nemá uživatel bez použití dodatečných nástrojů kontrolu prakticky žádnou a jeho soukromí je tak vydáno do rukou cizích společností. Může se tak stát, že tyto společnosti budou časem vědět o uživatelích více, než jejich blízcí. Aby nedošlo k naplnění této děsivé myšlenky, je potřeba své soukromí chránit.

Vyžadují-li uživatelé v prostředí internetu anonymitu a vysokou míru ochrany soukromí, jsou pro ně ideálními nástroji anonymizační sítě TOR či JonDonym. Při použití těchto sítí však může v rámci zachování maximální bezpečnosti dojít k omezení některých služeb (například na stránkách využívajících javové a flash objekty), což může pro některé uživatele představovat velký problém. Pokud uživatel nechce přijít o některé z výhod, které dnes různé webové služby nabízejí, stále existuje mnoho možností, jak se bránit monitorování a sběru informací cizími subjekty, aniž by k takovému omezení došlo. Tyto nástroje se velmi liší jak v použitých metodách ochrany (aktivní blokování – Ghostery, Do Not Track+, či pasivní - nastavování hlaviček DNT, opt-outs) tak v dostupnosti na různých platformách. Ačkoliv při jejich použití nedochází k omezení použitelnosti, již neposkytují tak komplexní ochranu jako výše zmíněné anonymizační sítě a jejich funkčnost je z pravidla omezena pouze na určité druhy hrozeb. Ideální úrovně ochrany soukromí lze tak v tomto případě

dosáhnout pouze jejich vhodnou kombinací, při které dojde k vzájemnému doplnění chybějících funkcí, při zachování plné funkčnosti jednotlivých komponent.

S aktivní ochranou před sledováním je potřeba začít co nejdříve, jelikož pasivní digitální stopy vznikají při každé nezabezpečené interakci s prostředím internetu. Je tedy velmi pravděpodobné, že každý uživatel má nějakou svou pasivní stopu, která vznikla ještě před využitím ochranných prostředků. Jak vyplývá z kapitoly 4.3, je velmi těžké, a v některých případech i nemožné, tyto stopy zpětně odstranit. Alespoň částečnou ochranu před růstem této stopy pak nabízejí nástroje na odstraňování již uložených sledovacích souborů. Přesto, že tuto funkci mají i běžné prohlížeče, nedokáží ochránit před všemi druhy těchto souborů (např. flash cookies). Uživatel má tak na výběr z několika nástrojů poskytujících ochranu, ať už přede všemi hrozbami (CCleaner) či pouze před některými (ATF Cleaner, Temp File Cleaner).

Stejně jako existuje mnoho hrozeb plynoucích ze vzniku digitálních stop, existuje i mnoho volně dostupných nástrojů, kterými lze těmto hrozbám předejít. Proto je třeba volbu nástrojů pečlivě zvážit tak, aby jejich kombinací bylo možné dosáhnout maximální možné míry ochrany soukromí při zachování požadovaných funkcí. Při správné kombinaci může dnes běžný uživatel tohoto stavu dosáhnout i s volně dostupnými nástroji.

Použitá literatura a zdroje

About Ghostery. EVIDON, Inc. *Ghostery* [online]. 2011 [cit. 2012-07-30]. Dostupné z: https://www.ghostery.com/about

About Tor: Overview. *Tor Project* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.torproject.org/about/overview.html.en

ACOHIDO, Byron. Facebook tracking is under scrutiny. *USA today* [online]. 11/15/2011 [cit. 2012-05-01]. ISSN 0161-7389. Dostupné z: http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1

AGGARWAL, Gaurav, Elie BURSZTEIN, Collin JACKSON a Dan BONEH. An analysis of private browsing modes in modern browsers. In: *Proceedings of the 19th USENIX Security Symposium*. Wahington, D.C., 2010, s. 79-94. Dostupné z: http://static.usenix.org/events/sec10/tech/full_papers/Aggarwal.pdf

ANGWIN, Julia. The Web's New Gold Mine: Your Secrets. *The Wall Street journal* [online]. July 30, 2010 [cit. 2012-01-04]. ISSN 00999660. Dostupné z: http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

ANGWIN, Julia. Web Companies Agree to Support 'Do Not Track' System. *The Wall Street journal* [online]. February 23, 2012 [cit. 2012-01-04]. ISSN 00999660. Dostupné z: http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html

Behaviorální marketing. In: *MediaGuru* [online]. 2012 [cit. 2012-04-28]. Dostupné z: http://www.mediaguru.cz/medialni-slovnik/behavioralni-marketing/

BITTO, Ondřej. Hesla na prodej. *Lupa*: *Server o českém internetu* [online]. 18. 5. 2005 [cit. 2012-01-04]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/hesla-na-prodej/

BlueKai Registry. *BlueKai* [online]. 2012 [cit. 2012-07-30]. Dostupné z: http://www.bluekai.com/registry/

CASEY, Eoghan. Computer Evidence and Computer Crime. In: PORADA, Viktor a Roman RAK. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. *Karlovarská právní revue*. 2006, roč. 2, č. 4, 1 - 21. Dostupné z: http://mail.vskv.cz/download/KPR/archiv/2006/kpr4_2006.pdf

ČERNÝ, Michal. Digitální stopy a digitální identita. *RVP*: *Metodický portál* [online]. 2011 [cit. 2012-04-28]. Dostupné z: http://clanky.rvp.cz/clanek/o/g/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html/

ČERNÝ, Michal. Digitální stopy. In: *E-bezpečí* [online]. 19.9.2011 [cit. 2012-01-04]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalni-stopy

Česko. Zákon ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000. Dostupné z: http://www.uoou.cz/files/101_cz.pdf

Česko. ZÁKON ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000. Dostupné z: http://www.uoou.cz/files/101_cz

DOČEKAL, Daniel. Flash Cookies - vlezlé, obtížně smazatelné a masově zneužívané. *Pooh* [online]. 16.8.2010 [cit. 2012-04-29]. Dostupné z: http://www.pooh.cz/IT/a.asp?a=2016280

DOČEKAL, Daniel. Google Profiles nabízejí miliony jmen i e-mailů uživatelů. *JustIT* [online]. 26/05/2011 [cit. 2012-05-01]. Dostupné z: http://www.justit.cz/wordpress/2011/05/26/google-profiles-nabizeji-miliony-jmen-i-e-mailu-uzivatelu/

DOČEKAL, Daniel. Hacknutý web ODS a data o členech z něj získaná podruhé. *Pooh* [online]. 2.4.2012 [cit. 2012-05-01]. Dostupné z: http://pooh.cz/pooh/a.asp?a=2017672

Download: Secure Cleaning. *Softpedia* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.softpedia.com/catList/98,0,1,0,1.html

Downloads tagged with: anonimity. *Softpedia* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.softpedia.com/downloadTag/anonimity

Egosurfing. In: *Techopedia*: *The IT Education Site* [online]. c2010 - 2012 [cit. 2012-05-05]. Dostupné z: http://www.techopedia.com/definition/26356/egosurfing

EMERY, Daniel. Details of 100m Facebook users collected and published. *BBC News* [online]. 29 July 2010 [cit. 2012-01-04]. Dostupné z: www.bbc.co.uk/news/technology-10796584

EVIDON, Inc. *Know Your Elements* [online]. c2011 [cit. 2012-05-14]. Dostupné z: http://www.knowyourelements.com/

Evropská Unie. Směrnice Evropského parlamentu a Rady 95/46/ESze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *Úřední věstník evropských společenství*. 23.11.1995. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:15:31995L0046:CS:PDF

FBI. Digital Evidence: Standards and Principles. *Forensic Science Communications* [online]. 2000, roč. 2, č. 2 [cit. 2012-04-28]. Dostupné z: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Definitions

FEDERAL TRADE COMMISSION. *About Identity Theft*: *Deter. Detect. Defend. Avoid ID Theft* [online]. 2012 [cit. 2012-05-01]. Dostupné z: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

FISH, Tony. *My digital footprint*: *a two sided digital business model where your privacy will be someone else's business* [online]. London: Futuretext, 2009 [cit. 2012-04-28]. ISBN 978-095-5606-984. Dostupné z: http://31.222.183.71/footprint-cms/THE_BIG_PICTURE.html

Get your Data: Make an Access Request at Facebook!. *Europe-v-Facebook* [online]. 2012 [cit. 2012-05-14]. Dostupné z: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html

Global Web Stats: June 2012. *W3Counter* [online]. June 2012 [cit. 2012-07-30]. Dostupné z: http://www.w3counter.com/globalstats.php?year=2012&month=6
GOOGLE. *Internetový obchod Chrome* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://chrome.google.com/webstore

CHAPMAN, Cameron. *Smashing magazine* [online]. June 11th, 2010 [cit. 2012-07-30]. Dostupné z: http://www.smashingmagazine.com/2010/06/11/how-to-permanently-delete-your-account-on-popular-websites/

Informační bezpečnost: Ochrana osobních údajů na internetu. *Elektra*: *Portál elektronických materiálů FF UK* [online]. 2011 [cit. 2012-07-30]. Dostupné z: http://elektra.ff.cuni.cz/ingram/informacni-bezpecnost/InfoBezpecnost.pdf

IP Check. *JonDonym*: *the anonymisation service* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://ip-check.info/?lang=en

JANČA, Jan. Sociální sítě a lidské zdroje. *Cognito*: *Prozraďte světu, kdo jste* [online]. 29. 12. 2008 [cit. 2012-05-01]. Dostupné z: http://www.cognito.cz/internet/socialni-site-lidske-zdroje/

KASÍK, Pavel. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. *Technet*: *Technika kolem nás* [online]. 19. listopadu 2009 [cit. 2012-05-01]. Dostupné z: http://technet.idnes.cz/cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka

Krádež identity a jak se jí bránit. *Bezpečný internet* [online]. [cit. 2012-05-01]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

Lotame Privacy Policy. *Lotame* [online]. November 2, 2011 [cit. 2012-07-30]. Dostupné z: http://lotame.com/legal

MADDEN, Marry. *Privacy management on social media sites*. Washington, D.C.: Pew Research Center's Internet & American Life Project, 2012. Dostupné z: http://pewinternet.org/~/media//Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf

MADDEN, Mary, Susannah FOX, Aaron SMITH a Jessica VITAK. *Digital Footprints: Online identity management and search in the age of transparency* [online]. Washington: Pew Internet & American Life Project, 2007 [cit. 2011-04-19]. Dostupné z WWW: http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Digital_Footprints.pdf
MALÝ, Martin. Widgety: Osvěžení pro vaše webové stránky. *Lupa*: *Server o českém internetu* [online]. 19. 8. 2009 [cit. 2012-01-04]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/widgety-osvezeni-pro-vase-webove-stranky/

MARTÍNEZ-CABRERA, Alejandro. Erasing all digital footprints 'impossible'. *San Francisco chronicle* [online]. San Francisco, Calif.: Chas. D. Young, July 6, 2010 [cit. 2012-05-14]. ISSN 1932-8672. Dostupné z: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/07/05/BU4V1E8D9V.DTL

MEDIATI, Nick. Lawsuit: Ad Network Could Be Tracking You With HTML5. In: *PCWorld*: *GeegTech* [online]. Sep 21, 2010 [cit. 2012-07-30]. Dostupné z: https://www.pcworld.com/article/205950/lawsuit_ad_network_could_be_tracking_you_with_html5.html
Mozilla Firefox 4 Beta, now including "Do Not Track" capabilities. MOZILLA. *The Mozilla Blog*: *News, notes and ramblings from the Mozilla project* [online]. February 8th, 2011 [cit. 2012-05-14]. Dostupné z: http://blog.mozilla.org/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/

PETERKA, Jiří. Cookie. In: *eArchiv*: *archiv článků a přednášek Jiřího Peterky* [online]. 2011 [cit. 2012-04-29]. Dostupné z: http://www.earchiv.cz/a96/a638k130.php3

Podmínky poskytování služeb. YAHOO!. *Yahoo! Info Center* [online]. 2012 [cit. 2012-07-30]. Dostupné z: http://info.yahoo.com/legal/cz/yahoo/utos/terms/

PORADA, Viktor a Roman RAK. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. *Karlovarská právní revue*. 2006, roč. 2, č. 4, 1 - 21. Dostupné z: http://mail.vskv.cz/download/KPR/archiv/2006/kpr4_2006.pdf

Privacy Policy. *BlueKai*: *About Us* [online]. March 21, 2012 [cit. 2012-07-30]. Dostupné z: http://www.bluekai.com/privacypolicy.php

Privacy Policy. *MediaMind* [online]. May 5, 2011 [cit. 2012-07-30]. Dostupné z: http://www.mediamind.com/privacy-policy

Privacy Policy. *Omniture*: *Privacy Center* [online]. May 7, 2012 [cit. 2012-07-30]. Dostupné z: http://www.omniture.com/en/privacy/policy

Prohlášení o právech a povinnostech. FACEBOOK. *Facebook* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.facebook.com/legal/terms

SINGEL, Ryan. Are You Ready for Web 2.0?. *Wired* [online]. 10.06.2005 [cit. 2012-04-28]. ISSN 1059-1028. Dostupné z: http://www.wired.com/science/discoveries/news/2005/10/69114

Slovníček nejdůležitějších pojmů. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ [online]. 2012 [cit. 2012-04-29]. Dostupné z: http://uoou.cz/uoou.aspx?menu=281&loc=455

SMITH, Richard M. The Web Bug FAQ. In: *Electronic Frontier Foundation*: *Defending your rights in the digital world* [online]. November 11, 1999 [cit. 2012-04-29]. Dostupné z: http://w2.eff.org/Privacy/Marketing/web_bug.html

Smluvní podmínky společnosti Google. GOOGLE. *Google*: *zásady a pravidla* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.google.com/intl/cs/policies/terms/regional.html

Soukromí a bezpečnost. MOZILLA CORPORATION. *Doplňky a aplikace Firefox* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://addons.mozilla.org/cs/firefox/extensions/privacy-security/?sort=users

Stahování informací. FACEBOOK. *Centrum náovědy* [online]. 2012 [cit. 2012-07-30]. Dostupné z: https://www.facebook.com/help/?page=116481065103985

SWALLOW, Erica. How Recruiters Use Social Networks to Screen Candidates: Infographic. *Mashable*: *The Social Media Guide* [online]. October 23, 2011 [cit. 2012-01-01]. Dostupné z: http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/

The Cloak: *free anonymous web surfing* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.the-cloak.com/

The Information That Is Needed to Identify You: 33 Bits. *The Wall Street journal* [online]. August 4, 2010 [cit. 2012-01-04]. ISSN 00999660. Dostupné z: http://blogs.wsj.com/digits/2010/08/04/the-information-that-is-needed-to-identify-you-33-bits/

The Ultimate Guide to the Invisible Web. *OEDB*: *Online Education Database* [online]. c2006-2012 [cit. 2012-05-06]. Dostupné z: http://oedb.org/library/college-basics/invisible-web

TOMEK, Lukáš. Anonymní surfování: na výběr máte z několika možností. *Lupa*: *Server o českém internetu* [online]. 19. 3. 2010 [cit. 2012-01-04]. ISSN 1213-0702.

Dostupné z: http://www.lupa.cz/clanky/anonymni-surfovani-na-vyber-mate-nekolik-moznosti/

Top 15 Most Popular Websites: July 2012. *EBizMBA*: *The eBusiness Knowledgebase* [online]. 2012 [cit. 2012-07-31]. Dostupné z: http://www.ebizmba.com/articles/most-popular-websites

TOP weby českého internetu: Průběžně aktualizovaný žebříček TOP českých webů, podle hodnocení serveru Siteinfo. *Siteinfo* [online]. 2012 [cit. 2012-07-30]. Dostupné z: http://www.siteinfo.cz/top-weby

V USA chtějí po zájemcích o práci heslo k Facebooku. *E15*: *Ekonomika, byznys, finance* [online]. 24.3.2012 [cit. 2012-05-01]. ISSN 1213-7693. Dostupné z: http://zpravy.e15.cz/byznys/technologie-a-media/v-usa-chteji-po-zajemcich-o-praci-heslo-k-facebooku-754670

VRBA, Marek. Proxy servery: jak se falšuje návštěvnost. *Lupa*: *Server o českém internetu* [online]. 26.1.2005 [cit. 2012-01-04]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/proxy-servery-jak-se-falsuje-navstevnost/

Vývoj počtu uživatelů. ATAXO. *Klabosení*: *Český a slovenský Twitter v číslech* [online]. 2012 [cit. 2012-05-01]. Dostupné z: http://www.klaboseni.cz/vyvojpoctu.php

Website privacy policy. *EXlate* [online]. October 2010 [cit. 2012-07-30]. Dostupné z: http://exelate.com/consumer-opt-out/website-privacy-policy/

WORLD ECONOMIC FORUM. *Personal Data: The Emergence of a New Asset Class*. 2011. Dostupné z: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

World Internet Users and Population Stats. *World Internet Usage News and Population Stats* [online]. 2012, April 26, 2012 [cit. 2012-04-28]. Dostupné z: http://www.internetworldstats.com/stats.htm

Seznam příloh