Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Ochrana soukromí uživatelů internetu

Bc. Tomáš Berber

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Tomáš Berber

Informatika

Název práce

Ochrana soukromí uživatelů internetu

Název anglicky

Internet users privacy protection

Cíle práce

Cílem diplomové práce je analyzovat typy osobních údajů dostupných z internetu a vytvořit systematické shrnutí nástrojů a metod pro tvorbu ochrany soukromí uživatelů v internetu.

Dílčí cíle diplomové práce jsou:
Identifikace online signálů, které jsou získávány a sledovány o uživatelích internetu, zejména pak osobních a citlivých údajů.
Vyhotovení souhrnu celkového množství nalezených signálů.
Na základě výsledků z výzkumu (ze souhrnu nalezených signálů) zpracování proaktivního a reaktivního přístupu obrany proti zneužívání osobních a citlivých údajů.
Vytvoření případové studie minimalizace nebo úplné eliminace výskytu osobních údajů autora z výsledku vyhledávání.

Metodika

V teoretické části budou definovány hlavní pojmy v oblasti týkající se tématu diplomové práce, bude provedena analýza způsobů sledování a shromažďování osobních údajů o uživatelích na internetu prostřednictvím vhodných nástrojů. Systematicky budou také shrnuty nejčastější důvody a dopady sledování osobních údajů na internetu.

V praktické části bude provedena identifikace online signálů, které jsou získávány a sledovány o uživatelích internetu, zejména pak osobních a citlivých údajů. Tato identifikace bude zpracována pomocí vhodných nástrojů v online prostředí. Pro každý nástroj bude popsáno, jaké informace je možné v daném nástroji získat.

Bude zpracován souhrn identifikovaných online signálů, který bude definovat, jaké osobní a citlivé údaje uživatelů jsou na internetu získávány a sledovány.

Na základě výsledků ze souhrnu bude vytvořen proaktivní a reaktivní přístup obrany proti zneužívání osobních a citlivých údajů v internetu. V proaktivním přístupu obrany se bude jednat o uchování anonymity uživatele v online prostředí a v reaktivním přístupu bude zpracována případová studie k minimalizování nebo úplné eliminaci výskytu osobních údajů autora z výsledku vybraného internetového vyhledávače.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

osobní údaje, internet, Google, ochrana, ÚOOÚ, behaviorální marketing, cookies, target marketing, bubble filter

---

Doporučené zdroje informací

DOMES, M. *Tvorba internetových stránek pomocí HTML, CSS a JavaScriptu.* Kralice: Computer Media, 2005. ISBN 80-86686-39-6.

KOŽÍŠEK, M. – PÍSECKÝ, V. *Bezpečně n@ internetu : průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

POLČÁK, R. *Právo na internetu : spam a odpovědnost ISP.* Brno: Computer Press, 2007. ISBN 978-80-251-1777-4.

SKLENÁK, V. *Data, informace, znalosti a Internet.* V Praze: C.H. Beck, 2001. ISBN 80-7179-409-0.

SUEHRING, S. *JavaScript : krok za krokem.* Brno: Computer Press, 2008. ISBN 978-80-251-2241-9.

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 18. 10. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 10. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 18. 03. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Ochrana soukromí uživatelů internetu" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2017 _____

Poděkování

Rád bych touto cestou poděkoval panu doktorovi Václavu Lohrovi za jeho odborné vedení, věnovaný čas a věcné připomínky, které mi poskytl k vypracování této práce. Pak bych také rád poděkoval panu inženýrovi Gerasimu Farafonovovi, který mi pomáhal svými připomínkami, radami i náměty při obtížích nebo otázkách, na které jsem při práci narazil. Mé poděkování patří též panu magistrovi Ladislavu Hejlíkovi za poskytnuté informace z ÚOOÚ a rodině za pomoc a podporu během studia.

Ochrana soukromí uživatelů internetu

Souhrn

Tato diplomová práce se zabývá ochranou soukromí uživatelů internetu. Jejím hlavním cílem je analyzovat typy osobních údajů dostupných z internetu a vytvořit systematické shrnutí nástrojů a metod pro tvorbu ochrany soukromí uživatelů v internetu. V teoretické části je provedena analýza způsobů sledování a shromažďování osobních údajů o uživatelích na internetu prostřednictvím vhodných technologií a shrnutí nejčastějších důvodů a dopadů sledování osobních údajů na internetu. V praktické části je provedena identifikace online signálů, které jsou získávány a shromažďovány o uživatelích internetu, zpracován souhrn identifikovaných online signálů a vytvořen soubor doporučení proaktivního a reaktivního přístupu obrany proti zneužívání osobních a citlivých údajů v internetu.

Klíčová slova: osobní údaje, internet, Google, ochrana, ÚOOÚ, behaviorální marketing, cookies, target marketing, bubble filter.

Internet users privacy protection

Summary

This thesis is concentrating on internet users privacy protection. Its main objective is to analyze as much types of personal data available on the Internet as possible and create a systematic summary of the tools and methods for improving of user privacy on the Internet. In the theoretical part reader can find analysis of methods of user tracking and their personal data collection. For this purpose different relevant technologies has been used and a summary of them, together with the most common reasons of user tracking and its impact on privacy analysis can be also find in theoretical part. In the practical part author concentrated on identification of online signals that are acquired and collected for internet users, analysis and summary of the identified signals and on a set of recommendations for proactive and reactive approach of protection against misuse of personal and sensitive data on the Internet.

Keywords: personal data, Internet, Google, protection, The Office for Personal Data Protection, behavioral marketing, cookies, target marketing, bubble filter.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V dnešní době existuje na světě jen málo míst, kde se člověk nesetká s internetem. Internet se stal základním stavebním prvkem zdravé ekonomiky, úspěšných národních i nadnárodních společností a také nedílnou součástí života lidí na zemi. Člověk zde může pohodlně zjišťovat informace z celého světa bez fyzického kontaktu s okolím.

Aktivně nebo pasivně o sobě lidé sdělují informace, které si světové korporace dokážou pomocí různých nástrojů získat a využívají je k dalším účelům. Dá se pak říct, že každý počítač připojený do internetu je na této síti monitorován různými nástroji. Běžný uživatel používáním internetu tak nevědomky poskytuje své osobní údaje a přichází o svoji anonymitu.

Hlavním důvodem shromažďování osobních údajů uživatelů na internetu je finanční zisk. Profit je generován například pomocí cílené reklamy na konkrétní skupinu uživatelů.

Všem těmto nepříznivým vlivům jsou lidé v internetu vystavováni dnes a denně. Na základě těchto skutečností se snaží své osobní údaje na internetu chránit. Proto ve své diplomové práci řeším problém ochrany soukromí uživatelů v internetu. Zaměřím se na proaktivní a reaktivní způsob obrany v internetu.

Cílem diplomové práce je analyzovat typy osobních údajů dostupných z internetu a vytvořit systematické shrnutí nástrojů a metod pro tvorbu ochrany soukromí uživatelů v internetu.

Teoretická část je zaměřena na analýzu způsobů sledování a shromažďování osobních údajů o uživatelích na internetu prostřednictvím vhodných technologií a na shrnutí nejčastějších důvodů a dopadů sledování osobních údajů na internetu. V praktické části je provedena identifikace online signálů, které jsou získávány a shromažďovány o uživatelích internetu, bude zpracován souhrn identifikovaných online signálů a vytvořen soubor doporučení proaktivního a reaktivního přístupu obrany proti zneužívání osobních a citlivých údajů v internetu.

První část práce je zaměřena na osobní a citlivé údaje, současnou situaci užívání internetu ve světě a v ČR a na výběr sledovacích nástrojů.

Ve druhé části diplomové práce je provedena analýza způsobů sledování a shromažďování osobních údajů o uživatelích na internetu prostřednictvím vhodných nástrojů. Jsou zde zdokumentovány sledovací technologie jako cookies, webové štěnice, etag, zombie cookies, evercookies, pluginy sociálních sítí, web storage, canvas fingerprinting a akcelerometr. Následně jsou uvedeny důvody a dopady shromažďování osobních údajů. V této části je představena personalizace, profilování uživatelů, behaviorální marketing a způsob využití pro společnosti Google, Facebook, ukázka analýzy Facebooku ve Wolfram Alpha a filter bubble.

V neposlední řadě pro zjištění jaké údaje jsou o uživatelích sledovány, jsou představeny Lightbeam, cookies v historii prohlížeče, Panopticlick, Clickclickclick.click, BrowserLeaks a společnosti Google, Youtube, Facebook, Instagram a Twitter. Na základě výsledků ze sledovacích nástrojů je vyhotoven souhrn celkového množství nalezených signálů.

Nakonec je podle výsledků ze souhrnu nalezených signálů vytvořen proaktivní a reaktivní přístup obrany proti zneužívání osobních a citlivých údajů v internetu. V proaktivním přístupu obrany se jedná o uchování anonymity uživatele v online prostředí. Je provedena konfigurace ochrany soukromí ve webovém prohlížeči Google Chrome, kde je konfigurována ochrana soukromí, soubory cookies, nastavení obsahu a údajů o prohlížení. Následně jsou vybrány programy pro ochranu osobních údajů a provedena konfigurace nastavení proaktivního přístupu na webových stránkách Google, Youtube, Facebook, Twitter a Instagram. Reaktivní přístup obrany obsahuje případovou studii k minimalizování nebo úplné eliminaci výskytu osobních údajů autora z výsledku vybraného internetového vyhledávače.

2 Cíl práce a metodika

Hlavním cílem diplomové práce je analyzovat typy osobních údajů dostupných z internetu a vytvořit systematické shrnutí nástrojů a metod pro tvorbu ochrany soukromí uživatelů v internetu.

Dílčími cíli diplomové práce jsou:

- identifikace online signálů, které jsou získávány a sledovány o uživatelích internetu, zejména pak osobních a citlivých údajů,
- vyhotovení souhrnu celkového množství nalezených signálů,
- na základě výsledků z výzkumu (ze souhrnu nalezených signálů) zpracování proaktivního a reaktivního přístupu obrany proti zneužívání osobních a citlivých údajů,
- vytvoření případové studie minimalizace nebo úplné eliminace výskytu osobních údajů autora z výsledku vyhledávání.

V teoretické části budou definovány hlavní pojmy v oblasti týkající se tématu diplomové práce, bude provedena analýza způsobů sledování a shromažďování osobních údajů o uživatelích na internetu prostřednictvím vhodných nástrojů. Systematicky budou také shrnuty nejčastější důvody a dopady sledování osobních údajů na internetu.

V praktické části bude provedena identifikace online signálů, které jsou získávány a sledovány o uživatelích internetu, zejména pak osobních a citlivých údajů. Tato identifikace bude zpracována pomocí vhodných nástrojů v online prostředí. Pro každý nástroj bude popsáno, jaké informace je možné v daném nástroji získat. Bude zpracován souhrn identifikovaných online signálů, který bude definovat, jaké osobní a citlivé údaje uživatelů jsou na internetu získávány a sledovány. Na základě výsledků ze souhrnu bude vytvořen proaktivní a reaktivní přístup obrany proti zneužívání osobních a citlivých údajů v internetu. V proaktivním přístupu obrany se bude jednat o uchování anonymity uživatele v online prostředí a v reaktivním přístupu bude zpracována případová studie k minimalizování nebo úplné eliminaci výskytu osobních údajů autora z výsledku vybraného internetového vyhledávače.

3 Teoretická východiska

3.1 Sledování a shromaždování osobních údajů

Účelem této kapitoly je definovat osobní a citlivé údaje. V další části je uvedena současná situace užívání internetu ve světě a v ČR. Nakonec jsou představeny důvody a výběr sledovacích nástrojů pro tuto práci, které budou následně sloužit pro analýzu způsobů sledování a shromažďování osobních údajů o uživatelích na internetu.

3.2 Osobní a citlivé údaje

V této podkapitole je vysvětleno, co jsou to osobní údaje, citlivé údaje a jaký orgán se stará o jejich ochranu.

Ochranu osobních a citlivých údajů udržuje Úřad pro ochranu osobních údajů (ÚOOÚ). ÚOOÚ dle zdroje [1] uvádí, že „*smyslem zákona o ochraně osobních údajů je Listinou základních práv a svobod zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života a neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno."*

Osobním údajem se dle § 4 písm. a) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016 rozumí „*jakákoliv 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."* [2]

Osobním údajem je jakákoliv informace týkající se určité fyzické osoby. Fyzická osoba se dá identifikovat na základě čísla, kódu a jiných prvků specifických pro jeho osobu. Tyto prvky mohu být fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identita. Mezi osobní údaje patří: jméno, příjmení, rodné číslo, adresa bydliště, email, telefonní číslo. Ze zákonné definice osobních údajů vyplývá, že za osobní údaj se dají považovat i další údaje, které umožňují člověka identifikovat, kontaktovat nebo dohledat. Jedná se o údaje fyzické (výška, váha, vzhled, barva vlasů), psychické (reakce člověka na různé podměty), ekonomické (příjmy, vlastní majetek, stabilní zaměstnání, dluhy), kulturní (zájmy, koníčky) nebo sociální (rodinný stav, vzdělání). [3]

Citlivým osobním údajem je dle § 4 písm. b) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016,„*osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.*" [2]

Google na svých stránkách dle zdroje [4] uvádí, že existují webové stránky, pro které se kategorizace pomocí sledovacích technologií nepoužívá, jako například online lékárny (zde existuje riziko vybudování profilu zdravotního stavu) a politické webové stránky (zde existuje riziko zjištění politické příslušnosti). Autor konzultoval s ÚOOÚ, zda Google opravdu neshromažďuje citlivé údaje a bylo mu řečeno, že se s takovým případem po dobu tří let doposud nesetkali.

Orgán Evropský inspektor ochrany údajů dle zdroje [5] říká, že společnost zpracovává osobní údaje v případě, že pomocí těchto údajů vyčleňuje osobu, bez ohledu na to, zda je určité jméno vázáno na data. Dle ÚOOÚ se jakékoliv zpracování údajů o určité osobě bere jako osobní údaj. Osobním údajem se rozumí jakýkoliv údaj, který vede k identifikaci člověka, a to dle § 4 písm. a) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016. Zpracování údajů je systematicky prováděná operace a musí se prokázat, a to dle § 4 písm. e) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016. [2]

V Evropě je zákon o ochraně osobních údajů hlavním právním nástrojem pro ochranu spravedlnosti a soukromí. Zákon o ochraně osobních údajů přiznává práva osob, jejichž údaje jsou zpracovávány a ukládá povinnosti stranám, které zpracovávají osobní údaje. Listina základních práv Evropské unie dle zdroje [5] uvádí, že osobní údaje musí být zpracovány k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveným zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny a má právo, aby byly rektifikovány. Dle § 5 odst. 4 Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016, musí být subjekt údajů informován o účelu zpracování jeho

osobních údajů včetně jeho souhlasu a správce musí být schopen souhlas prokázat po celou dobu zpracování. [2]

V případě cookies, které jsou nezbytné pro komunikaci nebo pro služby požadované uživatelem, není potřebný žádný souhlas uživatele. [5]

3.3 Současná situace užívání internetu ve světě a v ČR

Cílem této podkapitoly je ukázat, jak je problém ochrany osobních údajů obsáhlý. Je představeno, kolik lidí na světě a v ČR je připojeno k internetu, a jak je internet využíván.

Na světě žije přes 7,3 miliard lidí, z toho přes 3,675 miliard lidí má internet. To znamená, že přes 50% celosvětové populace má internet. Nejvíce uživatelů internetu má Asie, 1,8 miliardy, pak následuje Evropa s počtem 614 milionů lidí. V Evropě je připojeno k internetu internet celkem 73,9% populace, čímž po Severní Americe s 89% zaujímá druhé místo ve světě. Denně stráví na internetu v průměru každý uživatel 118 minut. [6] [7]

V ČR je na internetu zhruba 7,18 milionu lidí. V porovnání s celou reálnou českou populací (10,5 mil.) se jedná o 68 % všech obyvatel. V případě porovnání s běžnou populací nad 10 let (9,4 mil.) je na internetu 76% české populace. Za únor 2016 činil v ČR průměrný strávený čas na internetu 43:25 hod. [8]

3.4 Výběr sledovacích nástrojů

Cílem této kapitoly je vybrat a uvést důvody výběru sledovacích nástrojů, které následně slouží k analýze způsobů sledování a shromažďování osobních údajů o uživatelích na internetu.

***Obr. 1**: Počet uživatelů/návštěvníků webových stránek za měsíc září v roce 2016 (Zdroj: autor)*

Graf zobrazuje počet uživatelů/návštěvníků webových stránek za měsíc září 2016. Autor oddělil dva druhy webových stránek barvami modrou a oranžovou. Modrá barva znázorňuje sociální sítě a její aktivní uživatele. Aktivní uživatelé jsou uživatelé, kteří vykazují aktivitu minimálně jedenkrát do měsíce. Webové stránky Youtube a Google jsou zvýrazněny oranžovou barvou, protože nespadají do sociálních sítí. Autor pro analýzu jakým způsobem a jakými nástroji jsou uživatelé sledováni, vybírá webové stránky s největší návštěvností, z tohoto důvodu spojil sociální sítě s vyhledávačem Google. Z grafu je vidět, že nejvíce aktivních uživatelů má Facebook s 1,712 miliardy návštěv za jeden měsíc. Youtube má měsíčně přes 1,3 miliardy návštěvníků, Google přes 1,1 miliardy návštěvníků za měsíc, který tento vyhledávač používají. Ostatní sociální sítě jako WhatsAPP, Facebook Messenger, Instagram, Twitter a Google+ si autor zvolil z toho důvodu, že spadají do TOP 10 sociálních sítí v celosvětovém měřítku. [9] [10]

3.4.1 Google

Google dosahuje 3,5 miliardy vyhledávácích dotazů za jeden den, což činí přes 1,12 bilionu vyhledávacích dotazů za rok. V listopadu 2015 se společnost umístila na prvním místě jako nejnavštěvovanější multiplatformní webová služba v USA s 247 miliony amerických unikátních návštěvníků a tržním podílem ve výši 63,9% mezi provozovateli

vyhledávačů v USA. Příjem z reklamy činí 67,39 miliard dolarů a patří mezi druhého nejpopulárnějšího poskytovatele reklam s 82,2% na trhu v USA. Celosvětově používá tento vyhledávač přes 80% populace, v USA přes 86% obyvatel a v Evropě ve státech Německo, Itálie, Španělsko a Francie přes 90% obyvatel. Zajímavé je, že v ČR dosahuje Google přes 60%, více jak 25% zaujímá Seznam, i tak si ale drží v ČR první místo mezi vyhledávači. [5] [11] [12] [13]

3.4.2 Facebook

Celosvětově užívá Facebook 38,6% onlinové populace. Za listopad 2016 dosáhl Facebook 208,97 milionů unikátních návštěvníků, čímž zaujímá druhé místo v celosvětovém měřítku. V červenci 2016 měl 1,71 miliardy aktivních uživatelů, z toho 823 milionů přes mobilní telefon. Průměrně dosahuje ale přes 1,083 miliard aktivních uživatelů za jeden den. Odhaduje se, že v ČR je na Facebooku přes 4 miliony uživatelů, což z ní v této zemi dělá TOP 1, další sociální sítě již nedosahují takových výsledků, pro porovnání, počet účtů LinkedIn činí zhruba 450 tisíc, u Twitteru 300 tisíc (návštěvnost je o dvě třetiny nižší než počet účtů).

Příjmy Facebooku za první tři měsíce 2016 dosáhly 1,51 biliardy dolarů. Uživatelé zde stráví v průměru 20 minut za den a udělají zhruba 4 miliony Liků každou minutu. Jeho datový sklad zpracovává celkem 300 petabytů dat, z toho 4 petabyty přibývají nově každým dnem. Je zde více jak 250 miliard fotek. [14] [15] [16] [17]

3.4.3 Youtube

Youtube alespon jedenkrát použilo v Evropě 81% lidí, celosvětově 82%. Pokud by ho řadili mezi sociální sítě, byl by na druhém místě celosvětově za Googlem. Průměrný počet unikátních uživatelů měsíčně činí 128 milionů. V ČR dosahuje týdenní počet návštěv 5,5 milionů. [5] [15] [18]

3.4.4 Instagram

Účet na Instagramu má přes 30% celkových uživatelů internetu. Dosahuje 400 milionů aktivních uživatelů, z toho 75% uživatelů je mimo USA. Přes 60 % uživatelů se přihlásí alespoň jednou za den, čímž zaujímá po Facebooku druhé místo. Pro představu zpracovávaných dat obsahuje přes 40 miliard fotografií. V ČR má tato sociální sít přes 200 tisíc uživatelů, což není mnoho, ale patří do prvních 5 TOP sociálních sítí v ČR. [15] [19]

3.4.5 Twitter

Twitter má měsíčně přes 310 milionů aktivních uživatelů a 500 milionů Tweetů každý den. V ČR zaujímá s 300 tisíci uživateli pozici TOP 4 mezi sociálními sítěmi. [15] [20]

3.5 Technologie používané pro sledování uživatelů v internetu

Cílem této kapitoly je představení sledovacích technologií používaných pro sledování uživatelů v internetu. Jsou zde uvedeny cookies, webové štěnice, etag, zombie cookies, evercookies, pluginy sociálních sítí, web storage, canvas fingerprinting a akcelerometr.

3.5.1 Cookies

Cookie se v HTTP protokolu označuje jako malé množství dat, které je generované webovým serverem a uložené jako textový soubor v paměti klientského počítače nebo na pevném disku. [21] [22]

Webové stránky užívají cookies ke:

- sledování výrobků, které lidé nakupují,
- monitorování stránek, které člověk navštěvuje,
- shromaždování informací pro webové servery o produktech, o které se lidé zajímají pro prezentaci reklamních bannerů,
- sběru personálních informací, které člověk sdělil webové stránce a následně k udržení pro další návštěvu webové stránky,
- ověření přihlášení do webové stránky s validním uživatelským ID a heslem. [22]

Z výše uvedeného je vidět, že data uložená v cookie obsahují často osobní informace o jednotlivých uživatelích.

Struktura cookie

Pro popis struktury cookies je vytvořena tabulka.

Tabulka 1: *Struktura HTTP cookie (Zdroj: autor)*

Název pole	Obsah
Name	Název cookie. [23]
Value	Hodnota cookie. [23]
Domain	Pro jakou doménu cookies platí. [23]
Path	Omezení platnosti cookies pro určtitou cestu. [23]
Expires / Max-Age	Datum expirace hodnoty cookie. [23]
Size	Velikost cookie. [23]
HTTP	Může být cookie použito pouze přes HTTP, a nebo je povolena modifikace skriptovacích jazyků? [23]
Secure	Je komunikace přes tuto cookie provedena šifrovaným přenosem? [23]
SameSite	Nastavena ochrana proti CSRF a XSS? [24]

Tabulka zobrazuje strukturu HTTP cookie. Struktura HTTP cookie se skládá ze sedmi polí. První dvě pole jsou povinná, jedná se o název a hodnotu cookie. Dále je v cookie uložena informace o doméně, pokud není tento atribut vyplněn, použije se aktuální název domény. Dalším atributem je Path nebo-li cesta v rámci domény. V případě, že je Path nastaven na '/', platí v rámci celé domény. Expires / Max-Age udává datum platnosti hodnoty cookie. Pokud není atribut nastaven, je cookie smazáno se zavřením prohlížeče. V případě Session cookie je hodnota nastavena na Session. Size udává velikost celé cookie. Zaškrtnuté pole HTTP značí, že může být cookie použito pouze přes HTTP a není povolena modifikace Java Scriptu. Atribut Secure udává, že v případě, že je atribut zaškrtnut, komunikace přes tuto cookie musí být provedena šifrovaným přenosem HTTPS. SameSite představuje, že pokud není atribut nastaven, není nastavena ochrana proti CSRF a XSS. Same-site cookies je mechanismus pro definování jak mají být cookies zasílány přes doménu. Umožňují serverům zmírnit rizika CSRF a útokům úniku informací. Mohou být nastaveny od nejnižší po nejvyšší ochranu jako no restricted – bez omezení, Lax volně a nebo Strict striktně. [23] [24]

Pro příklad popisu struktury HTTP cookie jsem zvolil nástroj DevTools v prohlížeči Google Chrome.

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure	SameSite
APISID	if-40fmRkulzhVIA/AXgOevJICf2mMRdxw	.google.com	/	2017-12-05T22:33:25.737Z	40			

***Obr. 2**: Ukázka Third-party cookie ASPISID (Zdroj: autor)*

Obrázek ukazuje Third-party cookie ASPISID, které užívají Google Maps. Ze struktury cookie se dá vyčíst název cookie APISID, hodnota cookie, platnost pro doménu google.com, Path platí v rámci celé domény, datum expirace do 2017-12-05 s hodinou 22:33, velikostí 40 bytů, atribut HTTP není omezen a je tak povolena modifikace Java Scriptu, Secure udává, že komunikace není vedena šifrovaným přenosem, SameSite je nastaveno jako no restricted, bez omezení.

Funkce cookie

V první řadě je důležité uvést rozdíly mezi bezstavovým protokolem HTTP a stavovými cookies. Komunikace pomocí HTTP je bezstavový, což znamená, že v případě komunikace prohlížeče s webovým serverem je po ukončení spojení transakce zapomenuta. Pokud je spojení navázáno znovu, neví již webový server, že s prohlížečem dříve komunikoval. Řešením bezstavového HTTP protokolu jsou cookies, které fungují stavově. Pokud uživatel navštíví poprvé webovou stránku používající cookies, je na zařízení uživatele uložen textový soubor, cookie, kam si webový server uloží potřebné informace. Tento textový soubor obsahuje unikátní ID, aby bylo možné při dalších návštěvách uživatele identifikovat a použít uložené cookie. V zařízení uživatele je textovému souboru přiřazena webová doména a přesná URL cesta stránky, na základě které bylo cookie vytvořeno. Na základě těchto kroků prohlížeč ví, kdy má danou cookie použít. Při každé další návštěvě webové stránky si spolu prohlížeč s webovým serverem vyměňují potřebná data a ukládají je dodatečně do cookie na základě kroků, které uživatel provede. [24] [22]

Dělení cookie dle životnosti v zařízení uživatele

Cookies se dělí na session cookies a persistent cookies. Session cookies se nikdy neukládají na disk nebo na jiné úložné médium a tak nepředstavují pro uživatele potenciální hrozbu. Slouží ke správné funkčnosti webu a jsou odstraněny po zavření prohlížeče. Persistent cookies jsou uloženy na zařízení uživatele. Tyto cookies zůstávají v uživatelském počítači do té doby, dokud neskončí expirace nebo dokud nejsou odstraněny. Některé persistent cookies jsou programovány tak, aby se vypnuly po skončení určitého data. Když některé z těchto cookies skončí její životnost, webový prohlížeč je

odstraní. Některé persistentní cookies nemají žádné datum expirace nebo vyprší až za dlouhou dobu v budoucnu, takže mají tendenci se shromažďovat ve vlastním úložišti klientských zařízení. [22]

First-party cookie a Third-party cookie

First-party cookie (cookies první strany) je nastavena pod doménou webových stránek, na kterých se uživatel nachází. Pokud uživatel navštíví určitou webovou stránku a tato stránka nastaví na své doméně cookie, je tato cookie nazvána first-party cookie.

Third-party cookie je nastavena z jiné domény než z webové stránky, na kterou se uživatel připojí. Third-party cookies jsou často nastaveny webovou stránkou která přísluší rozsáhlým webovým firmám, které jsou schopny kombinovat data cookies z více stránek aby vytvořili profil, jaké stránky člověk navštěvuje. [22]

Flash cookie

Flash cookies, též nazývané lokálně sdílené objekty, jsou kousky dat, které mohou webové stránky pomocí Adobe Flash ukládat na uživatelský počítač. Flash cookies jsou používány a nastavovány Adobe Flash Playerem, který je instalován prakticky na každém počítači, na kterém běží filmy, videa a hry. Velikost flash cookie se pohybuje do 100 kB a může obsahovat nashromážděné personální data a výsledky vyhledávání uživatelů. [25] [26]

Uložení flash cookie funguje tak, že malý 2kb neviditelný flash segment je uložen do webového prohlížeče s webovou stránkou. To slouží za účelem, aby nahrál návštěvu s pomocí flash cookie. Dle zdroje [26] více než půl stránek v internetu užívá flash cookies. Na mnoha stránkách slouží flash cookies jako záloha pro HTTP cookies, které by mohly být odstraněny. [25] [26]

Supercookie

Super cookie je typ HTTP cookie, která je navržena tak, aby byla permanentně uložena v počítači uživatele. Oproti HTTP cookies je mnohem obtížnější super cookies detekovat a odstranit ze zařízení. Mohou ukládat a obsahovat jakékoliv informace o historii prohlížení. [27]

3.5.2 Webové štěnice

Webová štěnice nebo sledovací pixel je jedno pixelový obrázek vložený ve webové stránce nebo obsažený v emailových zprávách. Sledovací pixel je kvůli své velikosti pro webový prohlížeč takřka neviditelný a slouží ke sledování chování uživatelů na internetu. [28]

Sledovací pixel se nejčastěji používá k měření návštěvnosti webových stránek. Dokáže zaznamenat IP adresu počítače, typ a verzi používaného webového prohlížeče, URL navštívené webové stránky a obrázku, čas a datum kdy byla stránka a obrázek zobrazen, dříve navštívené webové servery a informace o cookies vztažené k webové stránce, kde je webová štěnice vložena. Sledovací pixel nepředstavuje bez synchronizace cookies s konkrétním uživatelem velké riziko. [29]

V emailu se webové štěnice používají ke zjištění, jaký email byl přečten, kdy byl přečten, dále je možné získat IP adresu příjemce a jak často byl email odeslán a přečten. Tak je možné sledovat úspěšnost reklamy. Web bug je možné synchronizovat s cookie ke konkrétnímu emailu. Synchronizace spojí identitu uživatelů při budoucí návštěvě webové stránky. Web bug detektory je možné nainstalovat, ale není možné web bug odstranit. [29]

Web bug může na webové stránce také generovat reklamy pomocí cookies třetích stran. V nevyžádaných emailech se webové štěnice používají pro monitorování počtu lidí, kteří email uvidí. [28]

3.5.3 Etag

Etag je obvykle hashovaná hodnota generovaná serverem, která je součástí HTTP protokolu pro World Wide Web. Je to jeden z několika mechanismů, kterým prohlížeč ukládá na disk uživatele cachovaný obsah stránek. V případě otevření webové stránky, webový server vrátí aktuální reprezentaci zdroje spolu s odpovídající hodnotou etag. Tato hodnota je umístěna v hlavičce odpovědi HTTP v poli etag. Po uložení do cache a v případě, že chce uživatel nově načíst stejnou URL adresu, zašle webovému serveru svoji dříve uloženou kopii etag spolu s požadavkem v poli "If-None-Match". Tuto kopii etag server porovná s aktuální verzí etag. Pokud se hodnoty etag nezměnily, může server poslat velmi krátkou odezvu s HTTP 304 Not Modified status. Status 304 informuje klienta, že jeho cachovaná verze je stále v pořádku a může se použít. Pokud se ale hodnoty etag neshodují, je třeba stávající etag nahradit za nový, aktuální. [30]

Tímto způsobem zasílání hodnot etagů se uživatel hlásí serverům, které monitorují jeho pohyb na internetu. Tato metoda sledování slouží jako alternativa cookie. [30]

3.5.4 Zombie cookies

Zombie cookie je HTTP cookie, která se automaticky znovu obnoví po jejím odstranění. Zombie cookie je znovu vytvořena pomocí technologie od společnosti Quantcast. Quantcast vytvořila flash cookies ke sledování uživatelů na internetu. Tyto flash cookies jsou pak použity k opětovnému vytvoření cookies v prohlížeči, čímž dochází k obnovení cookies ve webovém prohlížeči, kterým se říká zombie cookies. [31] [32]

Webové stránky užívají flash cookies pro požadavky jako je například nastavení úrovně hlasitosti, zapamatování uživatelských preferencí hudby. Uživatelé jsou sledováni dle svého jedinečného ID. Když se uživatel pokusí odstranit cookies po návštěvě webové stránky s technologií Quantcast, uživatelské ID je uloženo v úložišti přehrávače Adobe Flash. Quantcast program načte uživatelské ID a znovu použije, aby mohl sledovat historii prohlížení. [31] [32]

Hlavním účelem zombie cookies je uložení personálních informací uživatele pro marketingové aktivity. Tato technologie společnosti Quantcast je užívaná mnoha webovými stránkami k měření návštěvnosti webových stránek a sbírání osobních profilů webových návštěvníků. [31] [32]

3.5.5 Evercookies

Evercookie je aplikace vytvořená v JavaScriptu, která produkuje extrémně trvalé cookies v prohlížeči. Jejím cílem je identifikovat klienta i poté, co odstraní standardní cookies, flash cookies a jiné. Evercookie se vytváří tak, že jsou data cookies ukládány do několika typů paměťových mechanismů, které jsou k dispozici ve webovém prohlížeči. Pokud uživatel odstraní některé typy cookies, jsou znovu obnoveny jiným dostupným mechanismem. Cookies mohou být uloženy a následně obnoveny například z těchto zdrojů: standardní HTTP cookies, Local Shared Objects (Flash), HTML5 Session Storage, HTML5 Local Storage, HTML5 Global Storage, HTML5 Database Storage (SQLite) a jiné. [33]

3.5.6 Pluginy sociálních sítí

Sociální sítě používají různé pluginy ke sledování interakcí uživatele se sociální sítí. Facebook používá pluginy například To se mi líbí, Sdílet a komentáře, vložené příspěvky. Podobně funguje také Twitter (Tweety), Instagram a jiné sociální sítě. Pokud uživatel klikne na To se mi líbí, bude sdílet informace, psát komentáře nebo vkládat příspěvky, dá tak možnost serverům tyto informace o uživateli sbírat, sledovat a následně profilovat jeho osobu. [34]

Facebook uvádí, že v případě kliknutí na tlačítko To se mi líbí, obdrží tato sociální síť údaje, které zahrnují uživatelské ID, navštívený web, datum a čas a další informace související s prohlížečem. [35]

Další možností je, že pokud se uživatel přihlásí na Facebook nebo Twitter na počítači a poté začne vyhledávat na internetu, mohou sociální sítě shromaždovat informace o vyhledávání dokud se neodhlásí. Často ale sledování uživatele nepochází přímo ze sociální sítě, ale skrz sdílené aplikace jako například Facebooku Farmville, kterou si uživatel přidá do účtu. [34]

Facebook dále uvádí, že dokáže sledovat uživatele internetu, pokud je uživatel odhlášen z Facebooku a nebo dokonce nemá na této sociální síti ani účet. Stačí pouze navštívit webovou stránku s modulem pluginu pro sociální síť, v tomto případě webovou stránku s modulem To se mi líbí a Facebook obdrží údaje o navštíveném webu, datu a čase a další údaje související s prohlížečem. [35]

3.5.7 Web Storage

Web Storage je samostatná aplikace, lokální úložiště na straně klienta, kam si webová stránka může skriptem uložit libovolná data a následně je skriptem opět načíst. Přístup k datům je ale možný pouze z klientského počítače, nepřenášejí se na server. Web Storage definuje dvě lokální úložiště: Session Storage a Local Storage, které se od sebe liší svoji perzistencí. Local storage ukládá data v prohlížeči do té doby, dokud nejsou skriptem smazány. Session Storage ukládá data jen po dobu trvání Session/relace, to znamená do doby než je zavřena stránka nebo prohlížeč. Web Storage neurčuje velikost těchto úložišť, doporučená velikost je ale mnohem větší než u cookies, a to až 5 MB. [36] [37] [38]

Často je Web Storage srovnáván s cookies. Rozdíly oproti cookies jsou následující:

- Cookies jsou hlavně určeny pro data, jež si chce server uložit do klientského prohlížeče, posílají se v hlavičkách HTTP dotazů a odpovědi a velikost je omezená. [36]
- Web Storage je doručen na webovou stránku pouze v případě, zažádá-li o to uživatel, zatímco cookies jsou zasílány s každou HTTP žádostí. [36]
- Web storage může být zpřístupněn na straně klienta pouze JavaScriptem, zatímco cookies mohou být vytvořeny jak PHP na straně serveru, tak JavaScriptem na straně klienta. [36]
- Cookies jsou specifické pro prohlížeče a doménu, ale nedělají rozdíl mezi okny v tom samém prohlížeči, ale Web Storage (hlavně Session Storage) rozlišuje mezi okny prohlížeče a domény. [36]

Tak jako cookies, WebStorage může být napaden XSS útoky. Je psán v JavaScriptu, a tak je možné pomocí XSS posbírat data uživatele. [36]

3.5.8 Canvas fingerprinting

Canvas, nebo-li plátno, je HTML5 rozhraní, které se používá k vykreslení grafiky a animací na webové stránce pomocí skriptování v JavaScriptu. Plátno je možné použít ke snímání otisků webového prohlížeče a potažmo také pro jeho on-line sledování. [39] [40] [41]

Tato technika je založena na skutečnosti, že stejné plátno je možné zobrazit v různých počítačích. To se děje z několika důvodů. Na úrovni obrazového formátu se jedná o skutečnost, jak webový prohlížeč rozdílně zpracovává data, se kterými pracuje, jako obraz, export snímků a komprese. Konečný obraz může mít odlišný kontrolní součet, i když jsou pixely identické. Na systémové úrovni se jedná o operační systémy. Operační systémy mají různé fonty, které používají různé algoritmy a nastavení pro vyhlazování a renderování sub-pixelů. [39] [41]

Fingerprints je ale těžké blokovat, protože je není možné blokovat jak v nastavení webového prohlížeče, tak v anti-sledovacích zařízení jako Ad-Block Plus. Rich Harris, výkoný ředitel AddThis, řekl, že společnost začala testovat canvas fingerprinting začátkem roku 2014 jako alternativní cestu k nahrazení cookies. [39]

3.5.9 Akcelerometr

Studie [42] zjistila, že akcelerometry ve smartphonech a tabletech produkují unikátní otisk, který mohou firmy využívat ke sledování uživatelů. Akcelerometr je kus hardwaru, který měří stupně akcelerace zařízení, které je vloženo uvnitř zařízení. Pro smartphony a tablety je akcelerometr nástrojem, které umožňuje zařízení vnímat rotaci směru.

Studie věří, že unikátní otisky vznikají z hardwarových nedokonalostí při výrobě senzoru, při níž každý senzorový čip jinak reaguje na stejný pohybový stimul. Odlišnosti jsou tak nepatrné, že nemají vliv na většinu funkcí uživatele. Při bližším zkoumání vykazují tyto otisky odlišnosti, které se zjišťují na základě výpočtu residuálního součtu čtverců, průměru residuálního součtu čtverců, odchylek, shlukování a porovnávání šikmosti. [42]

Akcelerometry poskytovaly sice stejné výsledky, pokud se například měřil počet ušlých kroků, vektorové vlastnosti však měly odlišný otisk. Otisk akcelerometru nemusí promítat pokaždé stejný otisk určitého smartphonu. Záleží na operačním systému smartphonu, rozhraní pro programování aplikací, zatížení procesoru, to vše může ovlivnit naměřené hodnoty. [42]

Podobně jako akcelerometr, barometr a gyroskop mají také zabudované senzory pro snímání otisků, což nebylo předmětem této studie. Předmětem této studie bylo se zaměřit na akcelerometry. Google na svých stránkách udává, že informace o poloze mohou sledovat pomocí akcelerometru nebo gyroskopu, viz kapitola 4.1.65. [4] [42]

3.6 Důvody a dopady shromaždování osobních údajů

Cílem této podkapitoly je shrnutí nejčastějších důvodů a dopadů sledování osobních údajů na internetu. Nejprve bude představena personalizace, behaviorální marketing, profilování a pro demonstraci užití behaviorálního marketingu Facebook analýza ve Wolfram Alpha. Dále se tato subkapitola zabývá důvody a dopady shromažďování osobních údajů. Pro zjištění důvodů sledování údajů o uživatelích jsou vybrány stránky Google a Facebook. Kromě zřejmých dopadů, jakožto sledování a shromažďování osobních údajů, je vybrán filter bubble.

3.6.1 Personalizace

Personalizace vyjadřuje možnost přizpůsobit webovou stránku potřebám uživatele. Existují různé způsoby personalizace. [43]

V první řadě je to způsob statický, který umožňuje uživateli vybírat z různých předpřipravených grafických podob prezentace. Volba výběru je sice na uživateli, ale je omezena pouze na volbu mezi nabízenými grafickými podobami, nevytváří se na základě chování uživatele. Tato statická personalizace se vyskytuje například u různých freemailových služeb (přístup k poštovnímu serveru přes webové rozhraní jako například www.seznam.cz). [43] [44]

Druhým způsobem personalizace je dynamické přizpůsobení stránek zaměřené konkrétně na potřeby individuálního uživatele. Do této třídy patří v první řadě internetové portály, které tento způsob personalizace většinou používají k zobrazování aktuálních informací dle zadaných hodnot, například při vyhledávání počasí se zobrazí aktuální předpověď podle místa vyhledávání. [43] [44]

Další možností dynamické personalizace je schopnost upravovat obsah webových stránek podle uživatele, například skrývat některé informace či naopak přidávat informace z jiných zdrojů. Často se tato možnost objevuje s využitím RSS formátu. RSS kanály slouží pro upozorňování na nové zprávy na webových stránkách, které si uživatel přidal do kategorie sledovaných stránek. [43] [44]

Sofistikovanějším způsobem dynamické personalizace je přistupování ke každému uživateli odlišně, a to na základě jeho profilu vytvářeného v průběhu jeho interakce s vyhledávačem. Cílem vyhledávačů je získávání co největšího množství informací o konkrétním uživateli, tyto informace poté analyzovat a tím ho lépe obsloužit dle jeho potřeb. To se vytváří z toho důvodu, že se lidé raději vrací na vyhledávače, které korespondují s jejich zájmy a potřebami a tak i zvyšují návštěvnost webu. Filtrování výsledků vyhledávání se utváří na základě informací, se kterými server o uživatelích disponuje. Na jedné straně se dá tato skutečnost vnímat pozitivně, z druhé strany je často vnímána negativně. Negativně z toho důvodu, že má člověk pocit, že ho někdo na základě podstrčených reklam sleduje a shromažduje o nich informace. Tyto podstrčené reklamy mají člověka více stimulovat pro koupi produktů. [43] [44]

3.6.2 Behaviorální marketing

Behaviorální marketing provádí analyzování chování tak, že shromažďuje data o aktivitě uživatelů na internetu. Například sleduje odkazy, na které člověk klikne, co vyhledává, z jaké části země vyhledává a na jaké stránce web opustil. Na základě interakcí člověka s webovými stránkami je uživateli vytvořen na internetu profil chování, podle kterého pak počítačové algoritmy vybírají informace a reklamy. Tyto informace a reklamy pak korespondují se zájmy a požadavky, které člověk na internetu dříve vyhledával. [45]

Behaviorální marketing na internetu se dělí na:

- **Sledování chování uživatele na konkrétním webu** - zjišťují se informace, z jakých stránek se uživatel na web dostal, z jaké části země pochází, co ho na stránkách zajímá, jaké má na stránkách problémy a na jaké stránce web opustil. Na základě těchto informací je možné upravit design a strukturu stránek tak, aby co nejlépe splňovaly požadavky uživatele. [45]
- **Behaviorální cílení** - jedná se o reklamní systémy, které slouží k utváření skupin uživatelů podle jejich nedávného chování na internetu. Dělí se na tři druhy.
    a) Tento druh cílení sleduje, jaké kategorie jsou navštěvovány na velkých portálech (například auta, krása, zdraví) a pak dle navštívených sekcí zobrazuje reklamy.
    b) Druhou možností je profilování uživatele dle dřívějších vyhledávaných slov na internetu.
    c) Třetí možností je využívání kontextové reklamy. Tato reklama se zobrazuje na základě klíčových slov, která jsou obsažena v článcích na webových stránkách. [45] [46]

3.6.3 Profilování

Cílem online profilování je shromaždovat informace o uživatelích internetu za účelem formulování osobních profilů na základě jejich zvyků a zájmů. [47]

Online profilování je možné dělit do dvou kategorií: aktivní a pasivní sběr dat. Aktivní sběr dat shromažďuje informace o chování uživatelů na webových stránkách, například zjišťování IP adresy návštěvníků, čas strávený na určitých webových stránkách a

jaké stránky uživatel navštěvuje. Tato data se používají k určení chování uživatele na internetu a tím pak charakterizují jednotlivé návštěvníky nebo skupiny návštěvníků. Data ale musí být transformována do smysluplných proměnných, aby mohla být dále použita. V rámci pasivního sběru dat se jedná o informace, které nemohou být shromaždovány sledováním chování uživatelů na internetu. Pasivní informace jsou získávány pomocí všech různých formulářů, které musí návštěvníci vyplnit. Jedná se převážně o osobní a citlivé údaje. Na sociálních sítích například při registraci jméno, pohlaví, datum narození a jiné. [47]

Výsledné onlinové profily mají pak velkou hodnotu pro trh, protože se dále používají k identifikaci různých segmentů zákazníků. Každý rozdílný segment vyžaduje rozdílné marketingové přístupy. Online profily umožňují společnostem poznat potenciální zákazníky. [47]

V dnešní době je čím dál tím větším trendem profilování pomocí digitálních záznamů. Digitální záznamy slouží k odhadování osobních vlastností, jako je věk, pohlaví, sexuální orientace, politická orientace a jiné. Výhodou tohoto profilování je, že má univerzální charakter. To znamená, že není omezen jazykovými bariérami. Je tedy možné sestavit profil člověka pomocí vizuálního jazyka, a to z různého kulturního prostředí a národnosti. Fotografie, které uživatel ukládá na sociální sítě, mohou být použity k predikci jeho zájmů, preferencí a názorů. Je tedy možné vytvořit zájmový profil uživatele pomocí analyzování jednotlivých obrázků uživatele, které přidal a pak agregací znalostí o obrázcích a rozložení dle preferencí a skupin kam je uživatel zařadil. [48]

3.6.4 Facebook analýza ve Wolfram Alpha

Pro ukázku fungování behaviorálního marketingu si autor vybral Facebook analýzu ve Wolfram Alpha.

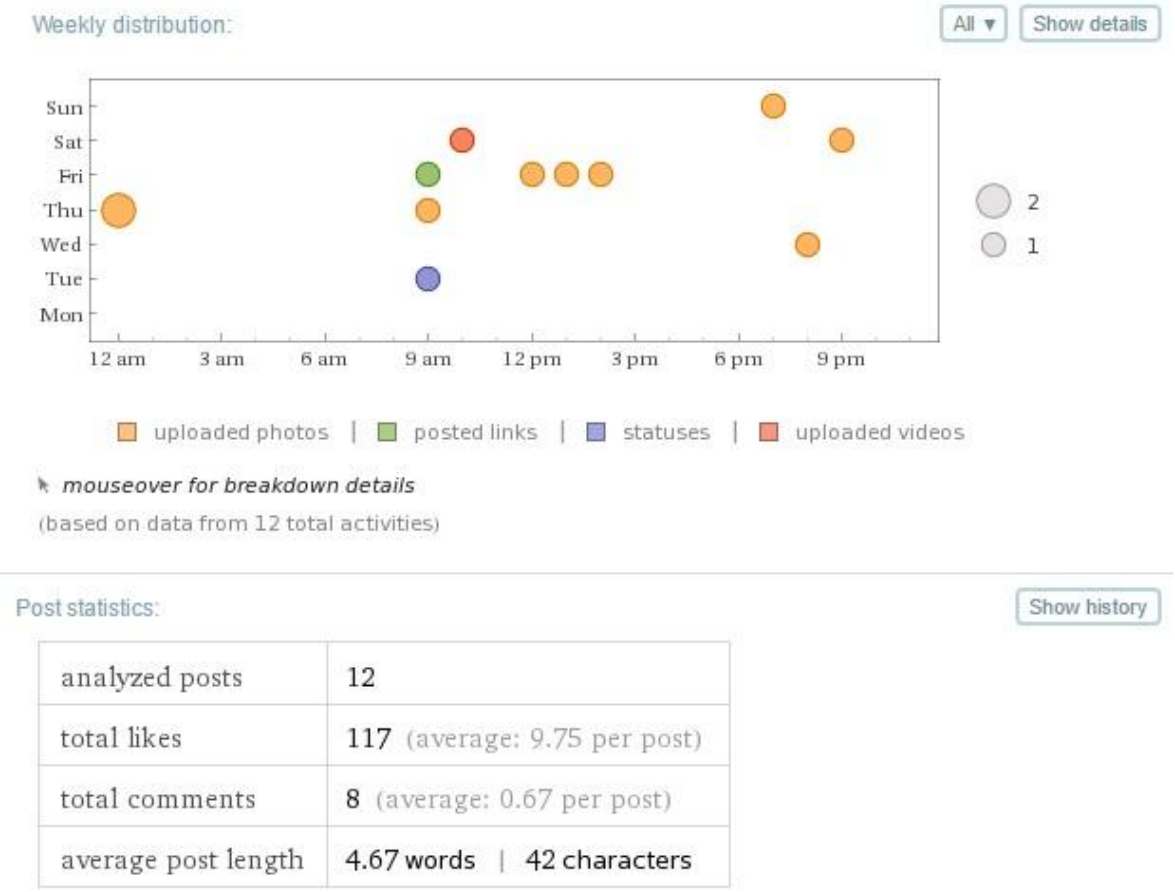
Wolfram Alpha je služba, která se snaží přímo odpovídat na dotazy uživatele. Tím se liší od vyhledávacích služeb, které poskytují pouze seznam stránek obsahující relevantní odpověď. Tato služba je vytvořena na základě výpočetního softwaru Mathematica, který je využíván pro řešení algebraických úloh, statistických a numerických výpočtů, ale i vizualizaci výsledků. [49]

Ve službě Wolfram Alpha existuje report pro Facebook, který dokáže vyhodnotit zajímavé informace o uživateli v případě, že této to této službě povolíte a přihlásíte se přes

ni na Facebook. Wolfram Alpha si získané informace ale neuchovává natrvalo, ale po jedné hodině je smaže. V prvé řadě tato služba ví uživatelovo jméno a příjmení, datum narození, věk a kdy má autor další narozeniny. Další report je ale zajímavější, a proto je zde zobrazen.

***Obr. 3**: Autorova aktivita na Facebooku – historie vkládání příspěvků a jejich podíl (Zdroj: autor)*

Obrázek popisuje autorovu aktivitu na Facebooku od listopadu 2015 až do listopadu 2016. Je vidět, kdy autor vkládal fotografie, kdy postoval linky, statusy a uploadoval videa. Největší aktivity jsou vidět v březnu a říjnu roku 2016. V dalším koláčovém grafu je vidět, že autor nejvíce preferuje vkládání fotografií, vkládání fotografií tvoří 75% celkové aktivity.



***Obr. 4**: Autorova aktivita na Facebooku dle jednotlivých dnů a statistika vkládání příspěvků (Zdroj: autor)*

Graf znázorňuje, jaké dny a v kolik hodin autor nejčastěji různé příspěvky vkládá. Kolik vkladů bylo analyzováno, kolik Liků, a komentářů. To slouží k tvorbě tzv. Word cloudu, který tvoří hesla, která autor na Facebooku používal. Tato hesla se poté použijí pro tvorbu cílené reklamy. Je také vidět s jakou frekvencí slova používá. Jaké fotografie byly nejvíce likovány autorovi a jaké posty nejvíce komentovány.

3.6.5 Google

V první řadě je důležité zmínit, že hlavním důvodem sledování a shromažďování osobních údajů je zisk.

Všechny zpracované vyhledávací dotazy Google ukládá. Pro profilování a behaviorální cílení využívá Google reklamní služby jako například AdWords, AdSense a Doubleclick Ad Exchange.

Google Adsense je reklamní síť, která automaticky zobrazuje reklamy textové, obrazové a videa na určitých webových stránkách, které odpovídají obsahu reklamy. AdWords představuje reklamu ve výsledcích vyhledávání Google, které si firmy kupují na základě PPC (pay-per-click). Reklamy se zobrazují v souladu s výsledky vyhledávání, což zajišťuje to, že jsou reklamy cíleny. [50] [51] [52]

Google zaznamenává data z cookies DoubleClicku jako čas a datum, kdy se uživatel díval na reklamu. Dále pak shromažďuje:

userid: unikátní ID cookie číslo, které získal uživatelův prohlížeč,
ad_id: unikátní ID reklamy,
ad_placement_id: ID kde byla reklama viděna na internetu,
referral_url: na jaké stránce uživatel byl, když viděl inzerát. [52]

Vzhledem k tomu, že zaznamenává také IP adresu uživatele, může dobře odhadnout zemi, město/vesnici, ze které byla reklama zobrazena. Dokáže říct, kolikrát uživatel reklamu viděl a například v jakém jazyce se má reklama zobrazit. Nemůže ale zjistit žádné osobní údaje o uživatelích. [52]

Pokud je cookie nastaveno na webové stránce které je součástí AdSence a uživatel vyhledává jinou stránku užívající AdSense, budou zaznamenány a vloženy ty samé informace. Později s nabývajícím množství údajů mohou být odhadnuty zájmy osoby, která prohlížeč používá. Tak se uživatel postupně škatulkuje do různých segmentů zálib, které umožnují DoubleClicku vybrat jaké reklamy se mají jakým uživatelům zobrazovat. Dále se DoubleClick snaží odvodit stát a věk uživatele pro lepší kategorizaci. [52]

Pokud chce uživatel vědět do jakého segmentu ho DoubleClick zařadil, je možné navštívit správce reklam. Zde se nachází jeho profil. O autorovi je zde uvedeno pouze pohlaví a odhadnutý věk v intervalu 25 – 34 let. [52]

Google uvádí, že shromážděné informace zpracovává ke zlepšení personalizace z toho důvodu, aby mohl uživatelům zobrazovat relevantnější výsledky vyhledávání a reklamy. Neshromažďuje údaje založené na rase, náboženství, sexuální orientaci nebo zdravotním stavu. Také uvádí, že se osobní údaje z jedné služby mohou spojit s informacemi z dalších služeb Google. Dále shromažďuje informace pro: vylepšení kvality služeb a vývoje nových služeb, zobrazování reklam na základě uživatelských zájmů

včetně věcí, jako jsou zadané vyhledávací dotazy nebo videa, která uživatel sledoval na Youtube, provádění analýz a měření pro zjištění jak jsou jeho služby používány. [50]

Při návštěvě webové stránky Googlu jeho servery automaticky zaznamenávají požadavky na stránky. Při vyhledávání tyto protokoly serveru často obsahují informace, jako je webový požadavek, IP adresa, typ prohlížeče, jazyk prohlížeče, datum a čas požadavku a jeden nebo více souborů cookie, které jednoznačně identifikují prohlížeč. [50]

3.6.6 Facebook

Do roku 2012 bylo zobrazování příspěvků řízeno speciálním algoritmem EdgeRank. Algoritmus určoval komu, kdy a jak příspěvky zobrazí. Postupem času EdgeRank nahradil nový komplexnější systém, který přistupuje ke každému uživateli individuálně a vychází z jeho aktivity a chování. Tento systém neustále vyvíjí a rozšiřují inženýři ze skupiny Feed Quality Panel. [53]

Facebook dále nabízí Core Audiences, umožňující rozdělení uživatelů do určitých kategorií. Tento nástroj pomáhá inzerentům kategorizovat uživatele dle lokace, demografickými zájmy nebo chováním. [46] [53] [54]

Pro představu jak je Facebook rozsáhlá síť jsou vybrány dvě zajímavosti. Na Facebook nahrávají uživatelé každou hodinu více než 10 milionů nových fotografií. Klepnutí na tlačítko líbí se nebo vložení komentáře proběhne přibližně 3 miliarda krát denně a zanechávají tak digitální stopu. [53] [54]

Facebook na svých stránkách [55] uvádí, že shromažďování údajů používá pro zlepšování služeb, personalizaci obsahu, vytváření relevantních návrhů a navrhování označení přátel na Facebooku. Testuje vyvíjené funkce a analyzuje získané informace pro vyhodnocování a vylepšení produktů a služeb, vyvíjení nových produktů a funkcí a řešení potíží. Dle zdroje [55] Facebook říká: „*Můžeme si rovněž ponechat informace z účtů deaktivovaných z důvodu porušení našich podmínek za poslední rok, abychom zabránili opakování zneužití či jiných porušení těchto podmínek.”*

3.6.7 Filter bubble

Filter bubble vzniká na základě personalizace uživatele a jeho interakce s webovými službami. Podle dříve vyhledávaných výsledků jsou pak uživateli podsouvána

témata, která jsou s jeho dřívějšími výsledky vyhledávání relevantní. Tímto způsobem je uživatel nedostává kompletní a nezaujaté informace. [56]

Eli Pariser tento termín popsal ve své knize [56], zde tvrdí, že webové služby mohou způsobit špatnou informovanost občanů o aktuálním dění ve světě. Tento problém může nastat v případě, že se online služby snaží zlepšit přesnost vyhledávání na úkor nezaujatosti dřívějšího vyhledávání, což vede k tomu co Pariser nazývá filter bubble. Pariser také uvedl příklad, ve kterém jeden uživatel v Google vyhledávači hledal termín "BP" a obdržel informace o investiční zprávě o British Petroleum, zatímco jiný hledající dostal informaci o úniku ropy z Deepwater Horizon. Pariser dále varuje, že filter bubble uživatele uzavírá do jakési bubliny vyhledávaných výsledků, čímž snižuje možnost přicházet na nové myšlenky, nápady a jiné důležité informace, vytváří dojem, že náš úzký vlastní zájem je vše, co existuje. V tomto ohledu kritizoval také Google a Facebook: „*World constructed from the familiar is a world in which there's nothing to learn ... (since there is) invisible autopropaganda, indoctrinating us with our own ideas*.“

4 Praktická část

4.1 Shromažďované údaje o uživatelích internetu

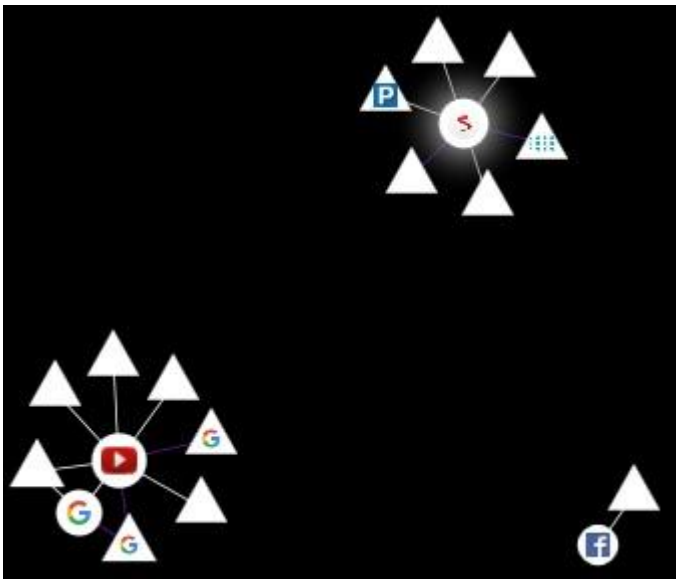
Cílem této kapitoly je identifikace online signálů, které jsou získávány a sledovány o uživatelích internetu, zejména pak osobních a citlivých údajů. Je představen doplněk Lightbeam, cookies v historii prohlížeče a nástroje Panopticlick, Clickclickclick.click, BrowserLeaks, také Google, Youtube, Facebook, Instagram a Twitter.

4.1.1 Lightbeam

Lightbeam je doplněk Firefoxu, který pomocí interaktivního modelu znázorňuje všechny stránky, se kterými uživatel na webu komunikuje. Zobrazuje vtahy mezi navštívenými stránkami a třetími stranami, které jsou na těchto stránkách aktivní. [57]

Tento test byl prováděn na prohlížeči Mozilla Firefox s odstraněnými cookies. Dle stránky níže si autor vybral na ukázku čtyři nejnavštěvovanější webové stránky v České republice, jedná se chronologicky o Facebook, Google, Seznam a Youtube. Ve světě si Youtube drží třetí pozici. [10]

Pro ukázku funkce Lightbeam si autor zvolil stránky: Google.cz, Youtube.com, Facebook.com a Seznam.cz.



***Obr. 5**: Vztahy mezi navštívenými stránkami a cookies třetích stran v aplikaci Lightbeam (Zdroj: autor)*

Obrázek ukazuje vztahy mezi navštívenými stránkami a cookies třetích stran v aplikaci Lightbeam. Při otevření vybraných stránek v pořadí Google.cz, Youtube.com,

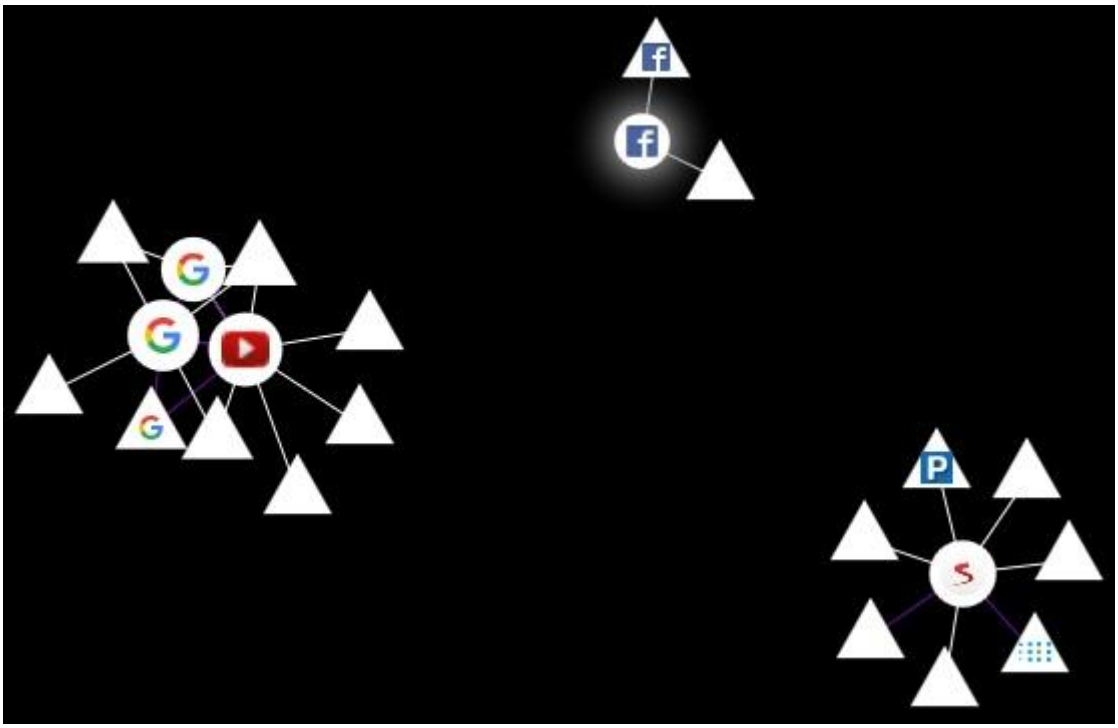
Facebook.com a Seznam.cz se zobrazí pavouk, graf spojení webových stránek. Je vidět, jak jsou stránky propojeny jak mezi sebou, tak s jinými cookies třetích stran, které při otevření příslušné stránky spolu navzájem komunikují. V grafu se spojil Google.cz s Youtube.com. Přímá interakce cookies je mezi Google.cz a Google.com, dále mezi Google.com a Youtube.com a mezi Seznam.cz a Imedia.cz a Gemius.pl. Níže graf znázorněn také v tabulce.

Tabulka 2: *Cookies třetích stran vybraných webových stránek v aplikaci Lightbeam (Zdroj: autor)*

Navštívená stránka	Third party	Spojení
Google.cz	google.com	Google.cz a Youtube.com
	gstatic.com	Google.cz a Youtube.com
Youtube.com	ytimg.com	Youtube.com
	ggpht.com	Youtube.com
	Doubleclick.net	Youtube.com
	Googlesyndication.com	Youtube.com
	Content.googleapis.com	Youtube.com
Facebook.com	akamaihd.net	Facebook
Seznam.cz	Imedia.cz	Seznam.cz
	Szn.cz	Seznam.cz
	Firmy.cz	Seznam.cz
	Gemius.pl	Seznam.cz
	Pubmatic.com	Seznam.cz
	Im.cz	Seznam.cz
	Mathtag.com	Nezobrazují se v grafu.
	Yahoo.com	Nezobrazují se v grafu.
	Adnsx.com	Nezobrazují se v grafu.
	Rfihub.com	Nezobrazují se v grafu.
	Adform.net	Nezobrazují se v grafu.
	Adsrvr.org	Nezobrazují se v grafu.
	Rlcdn.com	Nezobrazují se v grafu.

Tabulka ukazuje cookies třetích stran vybraných webových stránek (Google.cz, Youtube.com, Facebook.com a Seznam.cz) v aplikaci Lightbeam. Největší množství cookies třetích stran má webová stránka Seznam.cz, a to 13 cookies třetích stran. Po otevření těchto 4 vybraných stránek se ukázalo spojení mezi celkem 21 dalšími třetími stranami.

Dále se autor přihlásil na uživatelské účty do Google.cz, Youtube.com, Facebook.com a Seznam.cz.



***Obr. 6**: Vztahy mezi navštívenými stránkami a cookies třetích stran po přihlášení k uživatelským účtům v aplikaci Lightbeam (Zdroj: autor)*

Obrázek znázorňuje vztahy mezi navštívenými stránkami a cookies třetích stran po přihlášení k uživatelským účtům v aplikaci Lightbeam. Z obrázku je vidět, že z cookies třetích stran Google.com se stala přímo navštívená stránka, a to se autor do uživatelského účtu pouze přihlásil přes Google.cz. Přímé spojení mezi Google.cz a Google.com je v tuto chvíli zobrazováno jako při návštěvě obou stránek. Dále přibyly interakce mezi Google.com a cookies třetích stran. Nově zobrazované cookies třetích stran jsou vidět žlutě v tabulce níže.

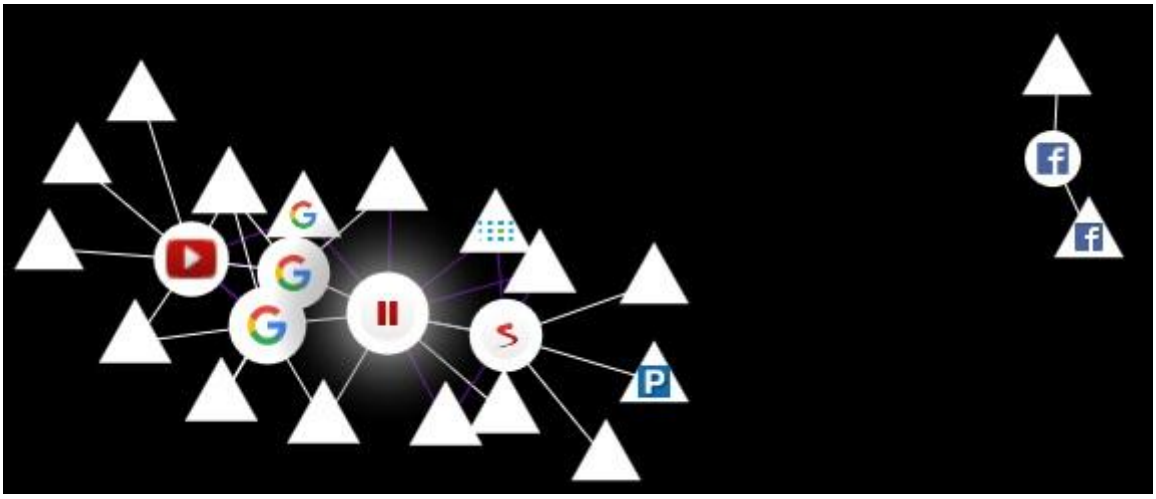
***Tabulka 3:** Cookies třetích stran vybraných webových stránek po přihlášení k uživatelským účtům v aplikaci Lightbeam (Zdroj: autor)*

Navštívená stránka	Third party	Spojení
Google.cz	gstatic.com	Google.cz a Youtube.com
	Googleusercontent.com	Google.cz a Google.com
Google.com	Google-analytics.com	
Youtube.com	ytimg.com	Youtube.com
	ggpht.com	Youtube.com
	Doubleclick.net	Youtube.com

Navštívená stránka	Third party	Spojení
	Googlesyndication.com	Youtube.com
	Content.googleapis.com	Youtube.com
Facebook.com	akamaihd.net	Facebook
	Fbcdn.net	Facebook
Seznam.cz	Imedia.cz	Seznam.cz
	Szn.cz	Seznam.cz
	Firmy.cz	Seznam.cz
	Gemius.pl	Seznam.cz
	Pubmatic.com	Seznam.cz
	Im.cz	Seznam.cz
	Post.cz	Seznam.cz
	Mathtag.com	Nezobrazují se v grafu.
	Yahoo.com	Nezobrazují se v grafu.
	Adnsx.com	Nezobrazují se v grafu.
	Rfihub.com	Nezobrazují se v grafu.
	Adform.net	Nezobrazují se v grafu.
	Adsrvr.org	Nezobrazují se v grafu.
	Rlcdn.com	Nezobrazují se v grafu.

Tabulka znázorňuje vztahy mezi navštívenými stránkami a cookies třetích stran po přihlášení k uživatelským účtům v aplikaci Lightbeam. Z tabulky je vidět, že nejvíce nových třetích stran přibylo u Googlu.cz, celkem 2 nové cookies třetích stran. Celkový počet stránek cookies třetích stran se zvýšil z počtu 21 na 24.

Dále autor do vyhledávače Google.cz zadal slovo zkouška, do Youtube.com spojení Mark Zuckerberg, tyto výrazy jsem zadal do vyhledávání. Na Facebook.com autor otevřel hlavní stranu a následně svůj profil. V poště Seznamu.cz klikl autor na tlačítko zpět a otevřel v Seznamu.cz video ve Stream.cz.



Obr. 7: *Vztahy mezi navštívenými stránkami a cookies třetích stran po přihlášení k uživatelským účtům při jejich užívání v aplikaci Lightbeam (Zdroj: autor)*

Obrázek ukazuje vztahy mezi navštívenými stránkami a cookies třetích stran po přihlášení k uživatelským účtům při jejich užívání v aplikaci Lightbeam. Na obrázku je vidět, jak jsou spolu vzájemně webové stránky propojeny a pomocí kterých cookies třetích stran. Pavučina spojení je mnohem rozsáhlejší a složitější než u výše testovaných propojení. Seznam.cz se pomocí Stream.cz spojil s Google.cz a Google.com. Pomocí vzájemných spojení cookies třetích stran společnosti získávají data a následně informace, které dále využívají ve svůj prospěch pro tvorbu reklamy.

Tabulka 4: *Cookies třetích stran vybraných webových stránek po přihlášení k uživatelským účtům při jejich užívání v aplikaci Lightbeam (Zdroj: autor)*

Navštívená stránka	Third party	Spojení
Google.cz	gstatic.com	Google.cz a Youtube.com
	Googleusercontent.com	Google.cz a Google.com
	Googleadservices.com	Google.cz
Google.com	Google-analytics.com	
Youtube.com	ytimg.com	Youtube.com
	ggpht.com	Youtube.com
	Doubleclick.net	Youtube.com
	Googlesyndication.com	Youtube.com
	Content.googleapis.com	Youtube.com
	2mdn.net	
	Fonts.googleapis.com	
	Moatads.com	
	Moatpixel.com	
Facebook.com	Akamaihd.net	Facebook
	Fbcdn.net	Facebook

Navštívená stránka	Third party	Spojení
Seznam.cz	Imedia.cz	Seznam.cz
	Szn.cz	Seznam.cz
	Firmy.cz	Seznam.cz
	Gemius.pl	Seznam.cz
	Pubmatic.com	Seznam.cz
	Im.cz	Seznam.cz
	Post.cz	Seznam.cz
	Mathtag.com	Nezobrazují se v grafu.
	Yahoo.com	Nezobrazují se v grafu.
	Adnsx.com	Nezobrazují se v grafu.
	Rfihub.com	Nezobrazují se v grafu.
	Adform.net	Nezobrazují se v grafu.
	Adsrvr.org	Nezobrazují se v grafu.
	Rlcdn.com	Nezobrazují se v grafu.
Stream.cz	Exiteria.cz	

Tabulka znázorňuje vztahy mezi navštívenými stránkami a cookies třetích stran po přihlášení k uživatelským účtům při jejich užívání v aplikaci Lightbeam. Z tabulky je vidět, že nejvíce nových třetích stran přibylo u Youtube.com, celkem 4 nové cookies třetích stran. Celkový počet stránek cookies třetích stran se zvýšil z počtu 24 na 30. V porovnání s pouze navštívenými 4 vybranými stránkami, kde počet cookies třetích stran činil 21, vzrostl počet cookies třetích stran po přihlášení na stránky a zadání jednoho požadavku na každé stránce o více jak 42%.

4.1.2 Cookies v historii prohlížeče

Před tímto testem autor smazal všechny cookies v prohlížeči Mozilla Firefox. V první řadě si autor znovu načetl všechny stránky jako v minulé subkapitole. Postupně Google.cz, Youtube.com, Facebook.com a Seznam.cz.

Pouze po otevření všech těchto 4 stránek se do prohlížeče Mozilla Firefox nahraje 50 cookies z 18 serverů. Je vidět, že největší množství cookies pochází ze stránky Seznam.cz. Je zajímavé, že po otevření stránky Facebook.com se žádné cookies do prohlížeče nenahraje, k nahrání 4 cookies dojde až v případě, že uživatel Facebooku odškrtne políčko s textem, že Facebook používá cookies.

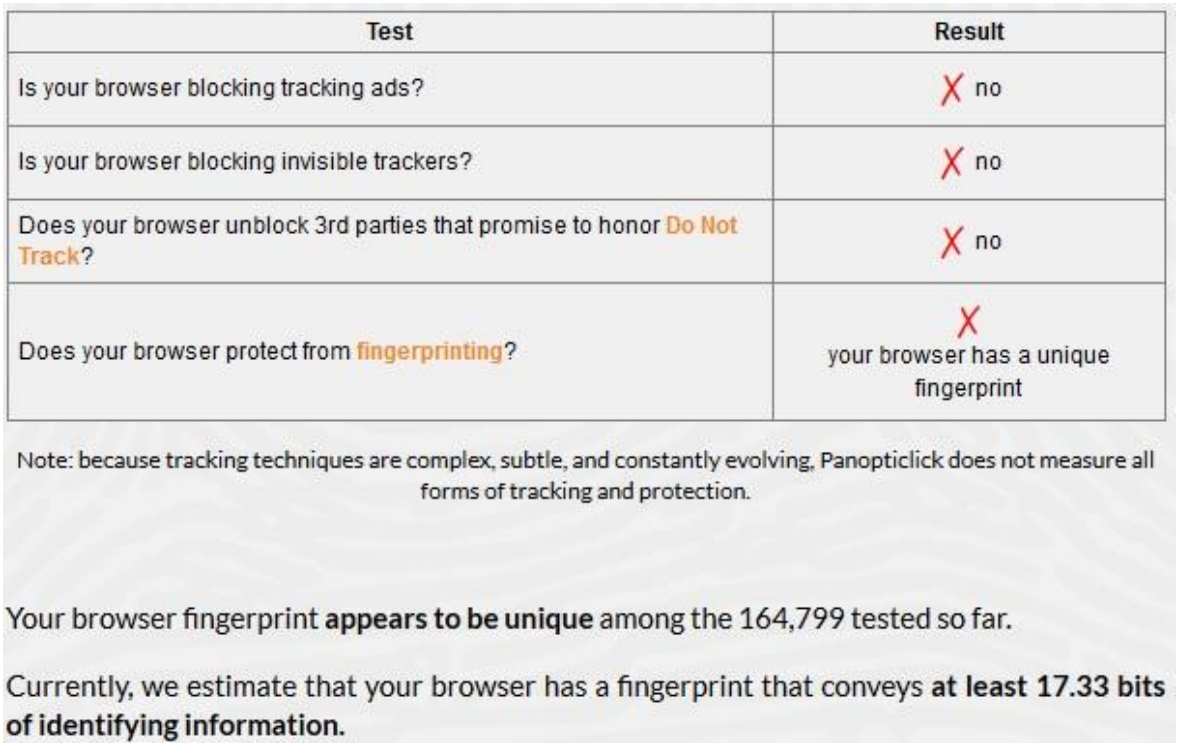
Při přihlášení pouze do Facebooku (zadání přihlašovacích údajů) jsou do prohlížeče Mozilla Firefox nahrány 12 cookies. Pokud se autor přihlásil dále do uživatelských účtů Google.cz, Youtube.com s Seznam.cz, do prohlížeče se nahrálo celkem 87 cookies.

4.1.3 Panopticlick

V této podkapitole autor čerpal ze zdrojů [58], [59] a [60].

Panopticlick je výzkumný projekt, který slouží k odhalení nástrojů a technik sledování uživatelů v internetu. Dále testuje účinnost zabezpečení soukromí instalovaných add-onů.

Pro testování autor zvolil prohlížeč Google Chrome s nejnovější aktualizací a bez jakékoliv ochrany.



Test	Result
Is your browser blocking tracking ads?	✗ no
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 164,799 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.33 bits of identifying information.**

***Obr. 8**: Testování ochrany zabezpečení v prohlížeči Google Chrome v projektu Panopticlick (Zdroj: autor)*

Obrázek znázorňuje testování ochrany zabezpečení v prohlížeči Google Chrome v projektu Panopticlick. Prohlížeč neblokuje sledující reklamy, neviditelné sledování, nemá povolené cookies třetích stran s nastavením Do Not Track, prohlížeč dále není chráněn před otiskem prohlížeče a má unikátní otisk prohlížeče.

Výsledek dále ukazuje, že stejný otisk prohlížeče jako autorův sdílí jeden ze 164 799 testovaných prohlížečů. Pro představení přesnosti výsledku dle zdroje [59] Panopticlick uvádí, že při testování ochrany soukromí mělo 83,6% uživatelů unikátní otisk.

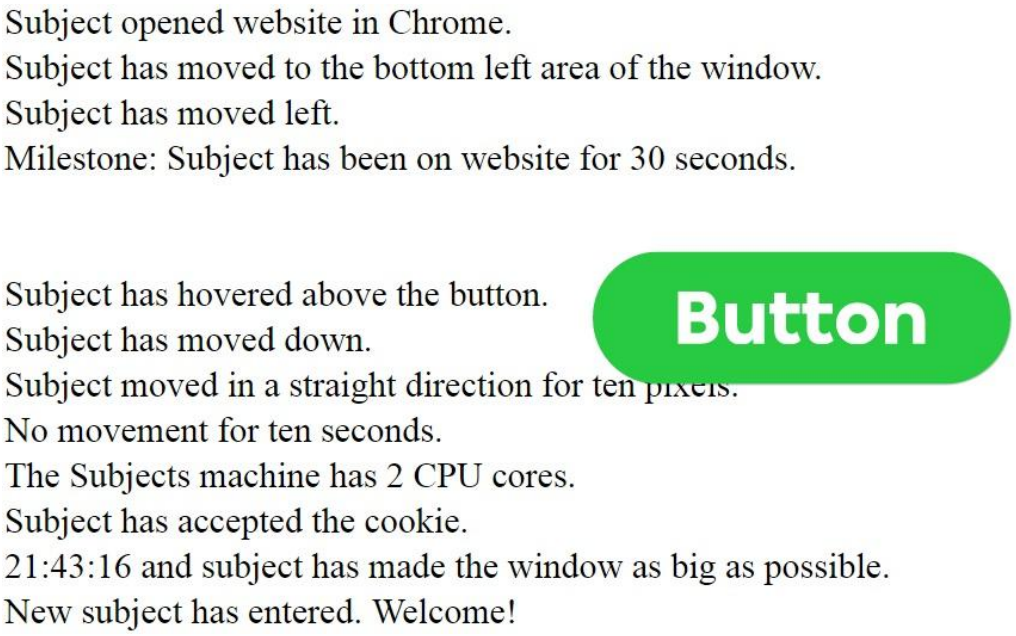
Panopticlick dále odhaduje, že testovaný prohlížeč má otisk, který zpracovává alespoň 17,31 bitů identifikačních údajů.

Další výsledky jsou v tabulce v příloze č. 1. Prohlížeč má povolené supercookies DOM localStorage a DOM sessionStorage. IE userData je hodnota nastavena na No, což znamená, že data o uživatelském profilu v zařízení nejsou poskytována.

Prohlížeč má dále unikátní hash v otisku prohlížeče s hodnotou0549f9b908d05b8b92b66c82d54f990c, velikost obrazovky a barevná hloubka. Browser dále poskytuje informace o instalovaných pluginech v prohlížeči, časové pásmo, hlavička Do Not Track je nastavena na false, dále co HTTP hlavička může přijmout, hash WebGL otistku prohlížeče je a4e41fd53affb34ce0b5e8dedf3399f4, jazyk nastaven český, jaké fonty jsou v počítači, platforma na jaké běží zařízení, co obsahuje User Agent, Touch Support je nastaven na hodnoty false, což je pravda na notebooku, zda jsou cookies povolené a jsou.

4.1.4 Clickclickclick.click

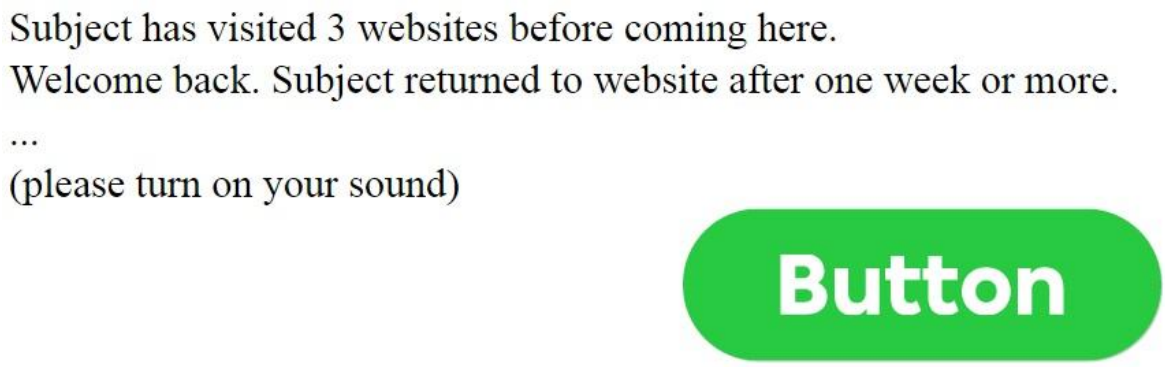
Clickclickclick.click byl vyvinut společností VPRO, holandskou mediální společností a Studiem Moniker, interaktivní designovou společností. Tato webová stránka ukazuje, jak je sledován každý pohyb uživatele na internetu. Sleduje detaily akcí v reálném čase a ukazuje to jak v písemné, tak vokální podobě. [61]



***Obr. 9**: Sledování interakce uživatele v prohlížeči Google Chrome v Clickclickclick.click(Zdroj: autor)*

Obrázek ukazuje sledování interakce uživatele v prohlížeči Google Chrome v Clickclickclick.click. Tato stránka dokáže zjistit, v kolik hodin subjekt navštívil tuto stránku, zda má otevřené velké okno, zda akceptoval cookies, kolika jádrový procesor je v počítači. Dále je vidět, jak se uživatel na stránce pohybuje, deset vteřin neprováděl žádný pohyb, jakým směrem se pohybuje kurzorem myši, jak dlouho na stránce je, jaký webový prohlížeč otevřel.

Autor opustil stránku Clickclickclick.clik a déle než týden se pohyboval na internetu a poté znovu otevřel Clickclickclick.clik.



***Obr. 10**: Sledování interakce uživatele v prohlížeči Google Chrome v Clickclickclick.click po více než jednom týdnu (Zdroj: autor)*

Obrázek ukazuje sledování interakce uživatele v prohlížeči Google Chrome v Clickclickclick.click po více než jednom týdnu. Tato aplikace sleduje také, kolik webových stránek uživatel po posledním otevření webového prohlížeče navštívil, v obrázku jsou to 3 webové stránky. Dále ukazuje, jak dlouho trvalo, než se uživatel na stránku znovu připojil, v tomto případě déle než jeden týden.

4.1.5 BrowserLeaks

BrowserLeaks je webová stránka, která představuje možnosti sledování uživatelů internetu. Jsou zde uvedeny informace jako IP adresa, informace o JavaScriptu prohlížeče, HTML5 Geolokace a otisk prohlížeče, vše je nížepodrobně představeno. V této podkapitole autor čerpal ze zdroje [62].

IP adresa uživatele

My IP Address :

IP address	188.175.125.133
Hostname	188.175.125.133

IP Address Location :

Country	Czech Republic (CZ)
State/Region	Hlavni mesto Praha
City	Prague
ISP	RIO Media a.s.
Organization	RIO Media a.s.
ASN	AS16246 RIO Media a.s.
Timezone	Europe/Prague
Local Time	Sat, 10 Dec 2016 14:19:13 +0100
Latitude/Longitude	50.1167, 14.6333

***Obr. 11**: Sledování IP adresy a lokace IP adresy v BrowserLeaks (Zdroj: autor)*

Obrázek ukazuje sledování IP adresy, Hostname a lokace IP adresy v BrowserLeaks. V lokaci IP adresy je vidět země, stát/region a město, kde se IP adresa nachází, poskytovatel internetových služeb, organizace, ASN, časové pásmo, místní čas a zeměpisnou šířku a délku.

Dále je na této stránce ukázáno, že možné zjistit technická data jako například informace o IP adrese WebRTC a Flash přehrávači, TCP/IP fingerprintu, DNS serveru a hlavičce HTTP.

Informace o JavaScriptu prohlížeče

JavaScript Detection :	
JavaScript Enabled	✓ True
Inline Scripts	✓ True
Same-Origin Scripts	✓ True
Third-Party Scripts	✓ True
Document Object :	
Document Referrer	https://browserleaks.com/
Screen Resolution	1366×768 16:9 24-bit TrueColor (working area: 1349×638)
Date/Time :	
System Time	Sat Dec 10 2016 14:56:04 GMT+0100 (Střední Evropa (běžný čas))
To Locale String	10. 12. 2016 14:56:04
To Locale Format	n/a
Navigator Object :	
userAgent	Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
appVersion	5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36

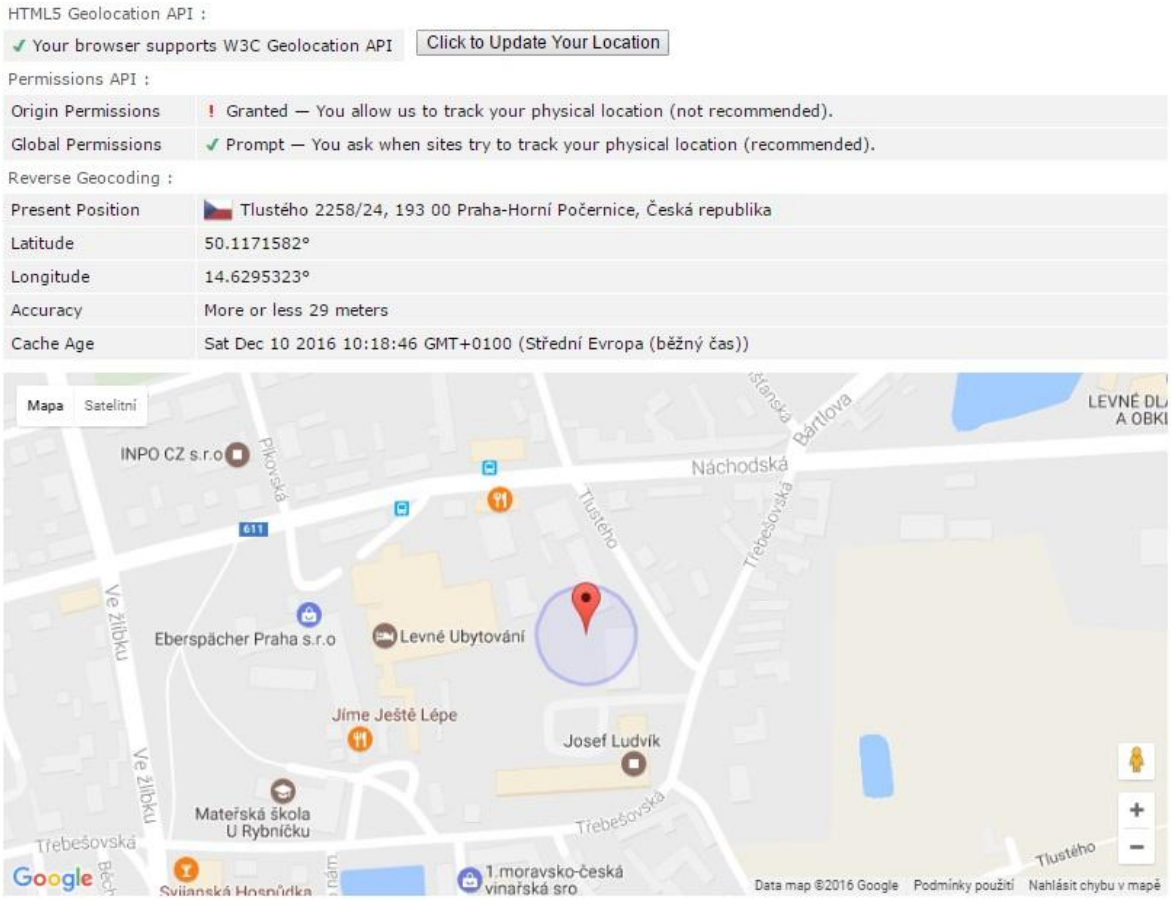
***Obr. 12**: Informace o JavaScriptu prohlížeče v BrowserLeaks (Zdroj: autor)*

Obrázek ukazuje informace o JavaSciptu prohlížeče jako dokument odkazujícího serveru, rozlišení obrazovky, datum, čas zařízení, User-Agent a verzi aplikací.

Dále je zde možné zjistit rozhraní stavu baterie a Web Audia, přístupové rozhraní, rozhraní o sítových informacích, instalované pluginy a navigační načasování rozhraní.

HTML Geolokace

Geolokační rozhraní je část standardu W3C HTML 5 a umožňuje webovým stránkám zažádat o fyzické umístění, čímž potenciálně ohrožuje soukromí uživatelů.



***Obr. 13**: Informace o HTML5 geolokaci v BrowserLeaks (Zdroj: autor)*

Obrázek znázorňuje, zda webový prohlížeč autora podporuje W3C Geolocation API, oprávnění k rozhraní, zda je umožněno sledovat uživatelovu fyzickou lokaci a v poslední řadě reverzní geocoding. V této části je vidět autorova adresa, zeměpisná šířka a délka, přesnost a čas, kdy byla lokace zjišťována.

HTML5 Canvas Fingerprinting

Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True
Canvas toDataURL	✓ True

Database Summary :

Unique User-Agents	160175
Unique Fingerprints	5900

Your Fingerprint :

Signature	✓ CE73D3E9
Found in DB	✓ True (3830 of 160175 unique User-Agents has the same signature as yours)
Image File Details :	BrowserLeaks.com <canvas> 1.0
File Size	5497 bytes
Number of Colors	599
SHA256	D3DC0344344626C2B5DAB5CF7BB849E43264BC231273EC5332E0B476BBF0EF24

PNG Headers	Chunk :	Length :	CRC :	Content :
	IHDR	13	477A703E	PNG image header: 220x30, 8 bits/sample, truecolor+alpha, noninterlaced
	IDAT	5440	CE73D3E9	PNG image data
	IEND	0	AE426082	end-of-image marker

Browser Detection :

✓ It is very likely that your web-browser is **Chrome** and your operating system is **Windows**.

***Obr. 14**: Otisk prohlížeče autorova prohlížeče v BrowserLeaks(Zdroj: autor)*

Obrázek ukazuje, zda autorův prohlížeč podporuje otisk prohlížeče, jedinečnost User-Agenta a unikátnost otisku prohlížeče, podpis autorova jedinečného otisku prohlížeče, zda byl nalezen v databázi (3830 z 160 175 jedinečných User-Agentů má stejný podpis jako autor, což činí 2,39%), jeho zobrazení, jedinečnost, velikost, otisk SHA256 a hlavičku PNG souboru. Je také vidět, že webová stránka ví, že autor používá prohlížeč Google Chrome a OS Windows.

Je možné zjistit jiné technické údaje jako údaje o WebGL, zda prohlížeč WebGL podporuje a obsah WebGL, dále údaje o Flash Playeru jako detekce Flashe, typ Flashe, rozšíření o další Flash pluginy, jaké fonty jsou na počítači instalovány a zda je ve webovém prohlížeči nastaveno Do Not Track.

4.1.6 Google

Při návštěvě webové stránky Googlu tento prohlížeč připomíná ochranu soukromí. Zde Google sděluje, jaké údaje shromažduje a zpracovává. Autor pro tuto podkapitolu čerpal ze zdroje [4].

Google shromažďuje následující informace:

Informace, které mu uživatel sdělí: Osobní údaje jako jméno, e-mailová adresa, fotografii, telefonní číslo nebo platební karta. Tyto informace Google uloží do uživatelského účtu.

Informace, které Google získá používáním jeho služeb: Shromažďuje informace o službách, které uživatel používá a jak je používá, to zahrnuje:

- **Informace o zařízení:** model hardwaru, verze operačního systému, jedinečné identifikátory zařízení, údaje o mobilní síti včetně telefonního čísla.
- **Informace z protokolu:** vyhledávací dotazy, informace z protokolu telefonování jako je uživatelské telefonní číslo, číslo volajícího, čísla přesměrování, čas a datum hovorů, doba trvání hovorů, údaje o směrování zpráv SMS a typy hovorů, adresa internetového protokolu; informace o událostech zařízení jako jsou selhání, činnost systému, nastavení hardwaru, typ prohlížeče, jazyk prohlížeče, datum a čas uživatelského požadavku nebo odkazující adresa URL; soubory cookies, které mohou být jedinečnými identifikátory uživatelského prohlížeče nebo účtu Google.
- **Informace o poloze:** polohu mohou určovat pomocí IP adresy, systému GPA a dalších senzorů (Zařízení může obsahovat senzory, které poskytují informace umožňující přesnější zjišťování polohy. Například pomocí akcelerometru lze zjistit rychlost a pomocí gyroskopu lze určit směr pohybu), které společnosti Google mohou poskytovat například údaje o zařízeních v okolí, přístupových bodech sítě Wi-Fi a vysílačích mobilních sítí.
- **Jedinečná čísla aplikací:** určité služby používají jedinečné číslo aplikace, které může být spolu s informacemi o instalaci nebo aktualizacemi odesláno Googlu. Jedná se například o typ operačního systému a číslo, verze aplikace.
- **Místní úložiště:** webové úložiště prohlížeče, mezipaměť aplikací, zde může Google shromažďovat a uchovávát informace včetně osobních údajů v místním úložišti uživatelského zařízení.
- **Soubory cookies a podobné technologie:** slouží k identifikaci prohlížeče nebo zařízení. Shromažduje a ukládá informace pomocí cookies, Third-party cookies například ze služby DoubleClick a využívá je například pro Google Analytics.

Google uvádí na svých stránkách příklad zpracování uživatelských údajů pro lepší pochopení. Když například uživatel vyhledává restauraci v Mapách Google nebo sleduje video na Youtube, zpracovává informace o této aktivitě, včetně údajů jako je sledované video, ID zařízení, IP adresy, data souborů cookies nebo poloha. Dále uvádí, že tyto informace zpracovává i v případě, když jsou používány aplikace nebo weby, které využívají služby Google, například reklamy, služby Google Analytics nebo přehrávač videí Youtube.

4.1.7 Youtube

Youtube sleduje historii vyhledávání uživatelů, aby mohl snáze personalizovat jejich domovskou stránku. Po načtení Youtube se zobrazují relevantní videa uživatele. Google je vlastníkem Youtube a tak se data ukládají do aktivní účtu Google. Když autor otevřel ochranu soukromí na Youtube, byl přesměrován na stránku se zásadami ochrany soukromí uživatelů Googlu, viz kapitola 4.1.6.

4.1.8 Facebook

Autor v této podkapitole čerpal ze zdroje [55]. Facebook na své stránce uvádí, jaké informace o uživatelích shromažďují.

Akce, které uživatel provádí a informace, které poskytuje: Shromažďují všechna data při používání Facebooku, včetně informací uvedených při registraci účtu, při vytváření nebo sdílení a posílání zpráv či jiné komunikaci s ostatními uživateli. Také sledují například místo pořízení fotky a datum vytvoření fotografie.

Akce, které provádí ostatní uživatelé a informace, které poskytují: Například při sdílení fotografie s více uživateli a následném označení uživatelů a napsání komentářů, to vše je importováno.

Sítě a spojení: S jakými lidmi je uživatel ve spojení, interakce s nimi, komunikace s lidmi ve skupinách, s kým sdílí obsah. Shromažďují informace také z adresáře zařízení.

Informace o platbách: Finanční transakce, když uživatel nakupuje na Facebooku nebo přispěje například na charitu, shromažďují informace o nákupu či transakci. Informace o platbě, číslo kreditní nebo debetní karty a další informace o kartě, další informace o účtu a ověření a také podrobnosti o fakturaci, dopravě a kontaktních údajích.

Informace o zařízení: Informace z počítačů, telefonů a dalších zařízení, na která uživatel instaluje nebo v nichž používá služby Facebooku a informace o těchto zařízeních. Informace získané z podpůrných zařízení mohou sdružovat.

Shromažďují operační systém, verzi hardwaru, nastavení zařízení, názvy, typy souborů a softwaru, výkon baterie, síla signálu a identifikátory zařízení. Umístění zařízení, včetně konkrétních zeměpisných umístění, například prostřednictvím GPS, Bluetooth nebo signálů Wi-Fi. Název mobilního operátora nebo poskytovatele internetových služeb, typ prohlížeče, jazyk a časové pásmo, číslo mobilního telefonu, IP adresa.

Informace z webů a aplikací, které využívají služby Facebooku: Například sdílení nebo tlačítko Like. Informace o webech a aplikacích, které uživatel navštěvuje, použití služeb na těchto webech a v těchto aplikacích, informace které poskytuje vývojář nebo vydavatel aplikace nebo webu.

Informace od externích partnerů a společností Facebooku (například Facebook Payments Inc, Instagram LLC, WhatsApp). Zde se jedná o cookies třetích stran.

Facebook ví o všem, co dělá člověk na internetu. Každá stránka, která obsahuje plugin s tlačítkem Like nebo Sdílej, zasílá chování uživatele na internetu zpět Facebooku, a to již od roku 2010.

4.1.9 Instagram

Autor pro tuto podkapitolu čerpal ze zdroje [63]. Od září roku 2012 vlastní Instagram společnost Facebook, která využívá nástroje třetích stran pro shromažďování a sledování uživatelů mezi sociálními weby.

Instagram shromažďuje údaje:

uživatelské jméno, heslo, e-mailovou adresu, informace o profilu (jméno a příjmení, obrázek, telefonní číslo), uživatelský obsah (fotky, komentáře), komunikaci mezi uživateli a Instagramem, jako například e-maily související s poskytováním služby (jako například e-maily související s ověřením účtu, změnou nebo aktualizací funkce služby, technická a bezpečnostní oznámení).

Sbírá také informace z protokolu jako je webový požadavek, IP adresa, typ prohlížeče, odkazující/konečné stránky adresy URL, počet kliknutí, způsob interakce

s odkazy ve službě, názvy domény, cílové stránky, zobrazené stránky, hastagy, geotagy, komentáře a jiné.

Ke sledování uživatelů používají cookies, analytické nástroje třetích stran, pixelové tagy, webové signály a místní úložiště. V rámci interakce Facebooku s Instagramem se shromážděná data prolínají.

Dle zdroje [63] Instagram uvádí, že *„společnost Instagram, její partneři nebo poskytovatelé služeb mohou údaje, které byly o vás shromážděny (včetně osobních údajů), převádět z jedné země do druhé a z vaší země nebo jurisdikce do jiných zemí nebo jurisdikcí po celém světě. Pokud se nacházíte v Evropské unii nebo dalších oblastech, kde se zákony o shromažďování a používání údajů mohou od zákonů Spojených států lišit, upozorňujeme, že údaje (včetně osobních údajů) můžeme převést do země nebo jurisdikce s jinými zákony na ochranu údajů, než jaké platí ve vaší jurisdikci...Poté, co svůj účet ukončíte nebo deaktivujete, může společnost Instagram, její partneři nebo poskytovatelé služeb uchovávat údaje (včetně informací o profilu) a uživatelský obsah pro komerčně přiměřenou dobu pro účely zálohování, archivace nebo auditování."*

Dle konzultace s ÚOOÚ je možné shromážděné údaje převádět mezi zeměmi volně pouze v rámci Evropské Unie, v jiném případě se o převodu údajů do třetích zemí má informovat ÚOOÚ, a to dle § 27 odst. 1 a 2 Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016. [2]

Co se týče uchování osobních údajů, a to dle § 5 odst. 1 písm. d) a e) Zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016, musí uchovavatel osobních údajů zdůvodnit, z jakého důvodu je shromažďuje a uchovávat je pouze po dobu, která je nezbytná k účelu jejich zpracování. [2]

4.1.10 Twitter

V této podkapitole čerpal autor ze zdroje [64].

Twitter sleduje:

Informace o uživateli: jméno, příjmení, datum narození, heslo, emailovou adresu, telefonní číslo, informace o platbách (čísla kreditní nebo debetní karty, datum vypršení platnosti karty, CVV kód, fakturační adresa a jiné informace o platbě, doručovací adresu),

fotografie, biografii, webové stránky, se kterými je uživatel propojen, demografická nebo zájmová data, obsah a interakce na webových stránkách nebo aplikacích.

Technické údaje: IP adresu, typ prohlížeče, operační systém, mobilního operátora, ID aplikace a zařízení a jiné.

Twitter získává tyto údaje při komunikaci s jejich službami a to i v případě, že nemá uživatel internetu vytvořený účet na Twitteru, postačí pouze používat jejich služby nebo instalovat aplikace přes Twitter.

Ke sledování využívají cookies jedné strany, cookies třetích stran, lokální úložiště, webové štěnice, klientské aplikace, přesměrování stránek, informace o přesné poloze z GPS, o Wi-Fi nebo mobilních vysílačích blízko používajícího mobilního zařízení. Důležité také je, že sice ctí nastavení Do Not Track v prohlížečích, ale používá Google Analytics.

4.2 Vyhotovení souhrnu celkového množství nalezených signálů

Cílem této kapitoly je vyhotovení souhrnu celkového množství nalezených signálů, které jsou o uživatelích sledovány a shromažďovány.

Souhrn se nachází v příloze č. 2. Signály jsou rozděleny do dvou hlavních skupin: údaje o uživateli a údaje o zařízení. Údaje o uživateli jsou dále rozděleny na osobní údaje, interakce s webovou stránkou a informace o poloze. Údaje o zařízení obsahují informace z protokolu mobilního telefonu a technické údaje. V každé podskupině se nacházejí konkrétní údaje.

4.3 Proaktivní přístup obrany

Cílem této kapitoly je na základě výsledků z výzkumu (ze souhrnu nalezených signálů) zpracování proaktivního a reaktivního přístupu obrany proti zneužívání osobních a citlivých údajů. V první části bude provedena konfigurace webového prohlížeče Google Chrome. Ve druhé části budou představeny programy pro ochranu osobních údajů. Další podkapitoly se věnují nastavení ochrany soukromí na Facebooku, Googlu, Youtube, Twitteru a Instagramu.

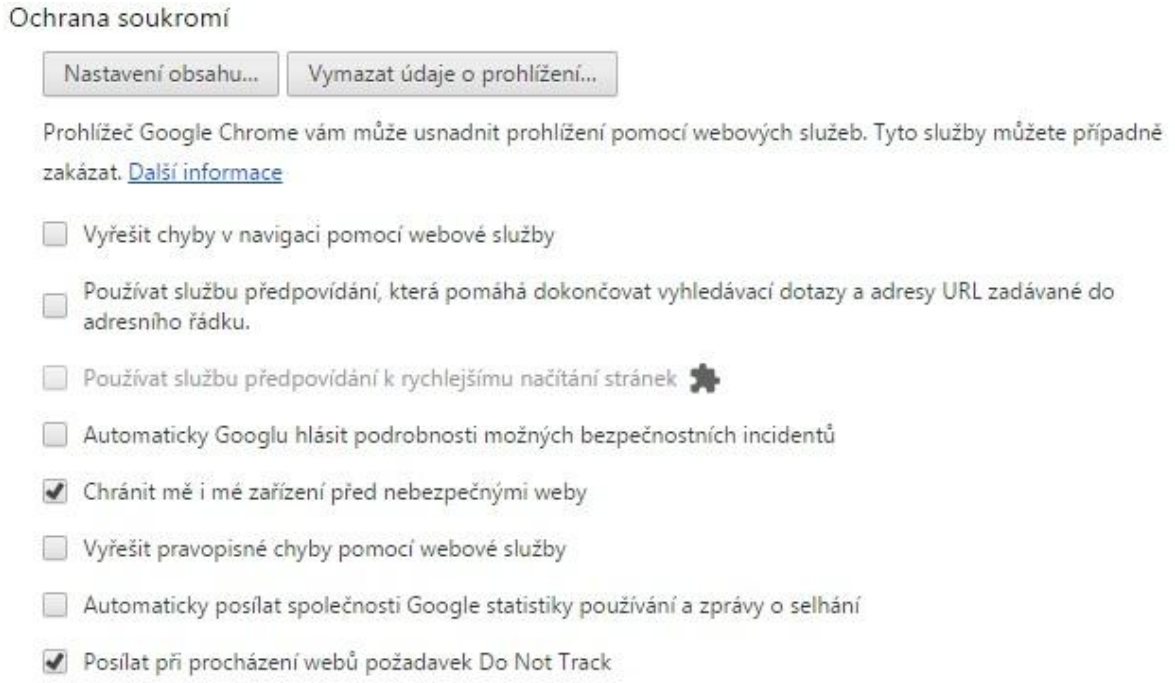
4.3.1 Konfigurace webového prohlížeče Google Chrome

V této podkapitole bude nastavena ochrana soukromí, souborů cookies, obsahu a údajů o prohlížení.

Ochrana soukromí

Cizí webová stránka může získat přístup k historii prohlížeče. Bude tak vědět, jaké webové stránky si uživatel prohlíží.

V první řadě autor nastavil ochranu soukromí webového prohlížeče Google Chrome.



***Obr. 15**: Nastavení ochrany soukromí v Google Chrome (Zdroj: autor)*

Obrázek zobrazuje nastavení jednotlivých možností ochrany soukromí, které je popsáno níže.

Vyřešit chyby v navigaci pomocí webové služby – pokud se uživatel nemůže připojit k určité webové stránce, jsou mu zobrazeny alternativní stránky podobné té, kterou vyhledává. Pro obdržení alternativních návrhů zašle Chrome do Googlu adresu webové stránky, kterou se uživatel pokouší najít. [65]

Používat službu předpovídání, která pomáhá dokončovat vyhledávací dotazy a adresy URL zadávané do adresního řádku nebo do vyhledávacího pole spouštěče aplikací – návrhy jsou založeny na souvisejících vyhledáváních na webu a historii prohlížení. Historie je vypnutá, z tohoto důvodu není potřeba tuto službu používat. [65]

Používat službu předpovídání k rychlejšímu načítání stránek – viz bod výše, historie je vypnutá, z tohoto důvodu není potřeba tuto službu používat. [65]

Automaticky Googlu hlásit podrobnosti možných bezpečnostních incidentů – neodesílat do Googlu informace o podezřelém stahování nebo webu. Chránit mě i mé zařízení před nebezpečnými weby – V případě návštěvy webových stránek s potenciální hrozbou, Chrome upozorní na toto nebezpečí. Vyřešit pravopisné chyby pomocí webové služby – Není nastaveno, Chrome odesílá zadaný text na servery Google. [65]

Automaticky posílat společnosti Google statistiky používání a zprávy o selhání – neodesílat statistiky využití a kolizí Googlu. [65]

Posílat při procházení webů požadavek Do Not Track – toto políčko je důležité, aby bylo zaškrtnuté a znamená nesledovat. [65]

Soubory cookie

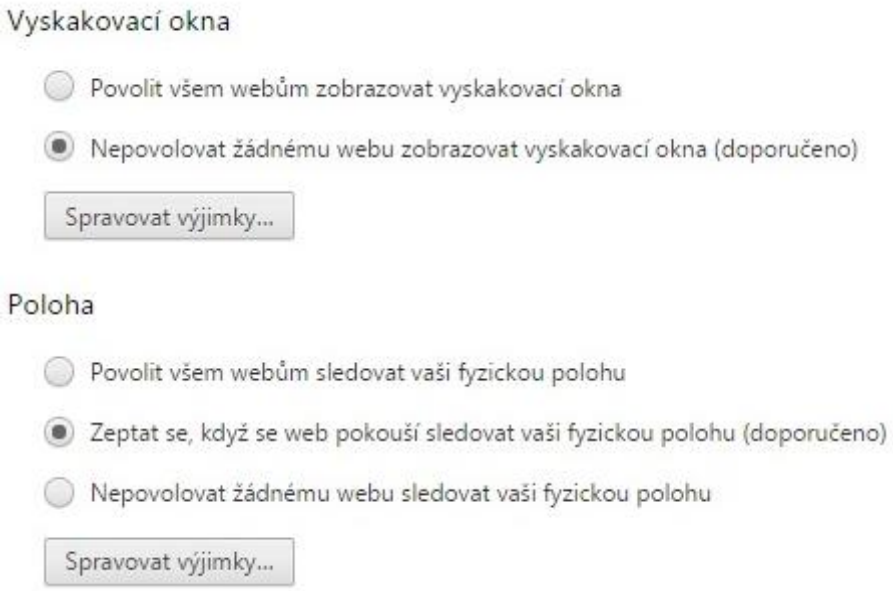
V této části jsou nastaveny soubory cookie.

***Obr. 16**: Nastavení souborů cookies v Google Chrome (Zdroj: autor)*

Obrázek ukazuje nastavení souborů cookies v prohlížeči Chrome. Je nastaveno, aby se místní údaje/cookie uchovávali jen do zavření prohlížeče, dále jsou blokovány soubory cookies třetích stran a data webových stránek.

Nastavení obsahu

V této části je provedeno nastavení obsahu.

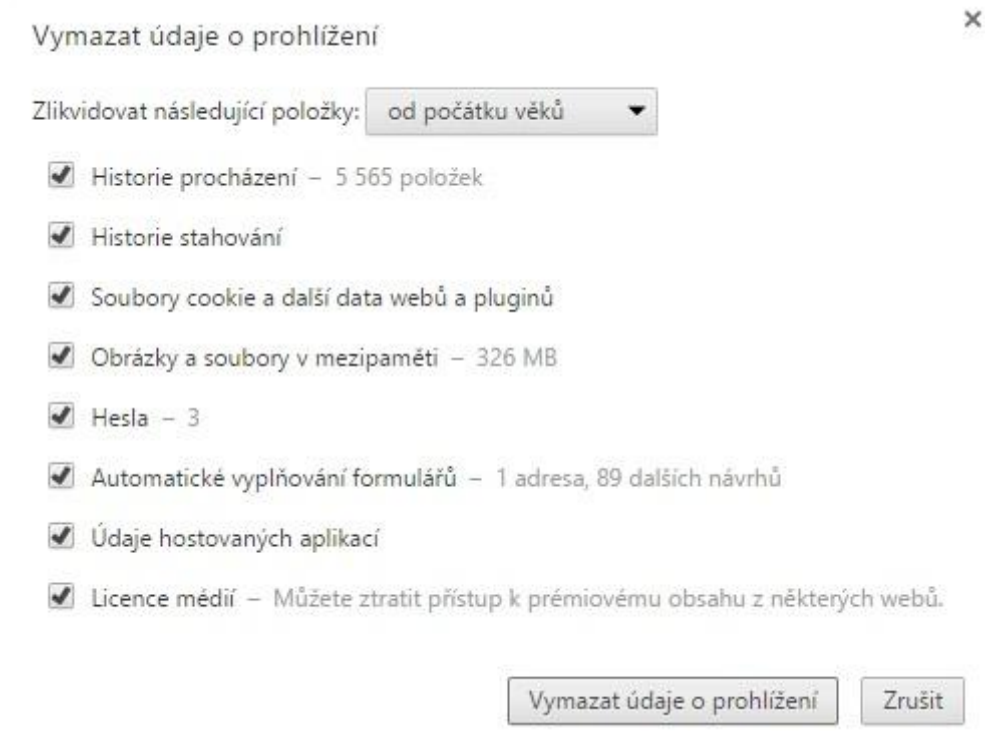


Obr. 17: *Nastavení obsahu v Google Chrome (Zdroj: autor)*

Obrázek ukazuje důležitá nastavení obsahu. Zde autor uvádí dvě důležité konfigurace. Nepovolovat žádnému webu zobrazovat vyskakovací okna a zeptat se, když se web pokouší sledovat fyzickou polohu zařízení. [66]

Údaje o prohlížení

Tato podkapitola se zabývá údaji o prohlížení.



***Obr. 18**: Smazání údajů o prohlížení v Google Chrome (Zdroj: autor)*

Obrázek znázorňuje vymazání údajů o prohlížení. Jsou dvě možnosti ochrany osobních údajů při používání webového prohlížeče. Google Chrome umožňuje neukládat historii pouze v anonymním režimu. Při používání anonymního režimu ale uživatel není na internetu neviditelný. Prohlížeč stále odesílá údaje do internetu včetně veřejné IP adresy. Druhou možností je každodenní mazání kompletní historie prohlížeče. Ta smaže historii procházení, historii stahování, soubory cookie a další data webů a pluginů, obrázky a soubory v mezipaměti, hesla, automatické vyplňování formulářů, údaje hostovaných aplikací a licence médií.

4.3.2 Programy pro ochranu osobních údajů

Typické ad blockery jsou provozovány jako nadstavba webových prohlížečů. Jak uživatel prochází internet, porovnávají požadavky navštívených stránek s jejich seznamem hostitelů (s hostujícími odkazy) a selektivně filtrují reklamy, trackery a jiné. To napomáhá chránit soukromí uživatelů při surfování, zabranuje útokům malwarů a snižuje požadavky na šířku pásma.

Pro ukázku ochrany osobních údajů autor vybral tři programy: AdBlock, Ghostery a uBlock Origin. Programy nebyly vybrány nahodile, ale na základě výsledků testování ad blockerů ze zdroje [67]. Testovalo se: doba načtení webové stránky, peak paměti při načítání a peak CPU při načítání. Tyto tři programy dosahovaly nejlepších výsledků.

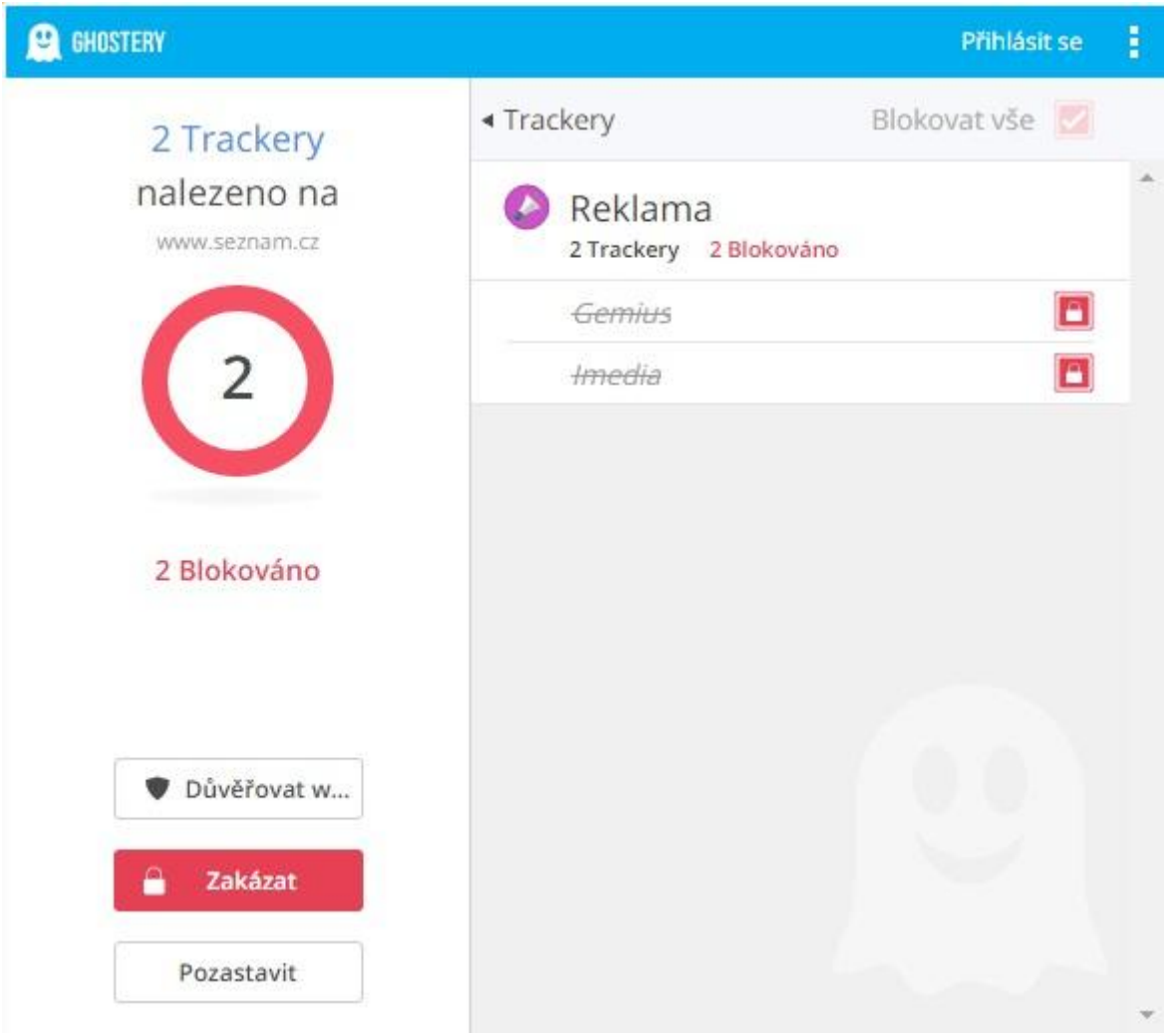
AdBlock (dostupný pro Chrome, Safari a Opera)

Nejpopulárnější rozšíření pro Chrome s více než 40 miliony uživateli a má přes 200 milionů stažení. Umožňuje filtrovat obsah načítaných stránek tak, aby s načtenými stránkami nenačítal reklamu a tím omezil přenos přenášených dat, šetřil pamět a CPU a stránka se zobrazila rychleji v té formě, jak si uživatel omezení filtrů přizpůsobí pro vlastní potřebu. Je možné přesně vybrat, jaké reklamy chce na určitých stránkách uživatel blokovat, pozastavit reklamu na konkrétní stránce nebo úplně pozastavit toto rozšíření. Byl vybrán z toho důvodu, že je nejrozšířenější a jeho průměrná doba načtení stránky činí 3,7 sekundy. Pro porovnání s nejrychlejším uBlock Origin, s 3,2sekundy je to srovnatelné. Jeho záporná stránka je, že využívá velké množství paměti, až 100 MB a až na 15,4% využívá CPU. [68]

***Obr. 19**: AdBlock v Google Chrome (Zdroj: autor)*

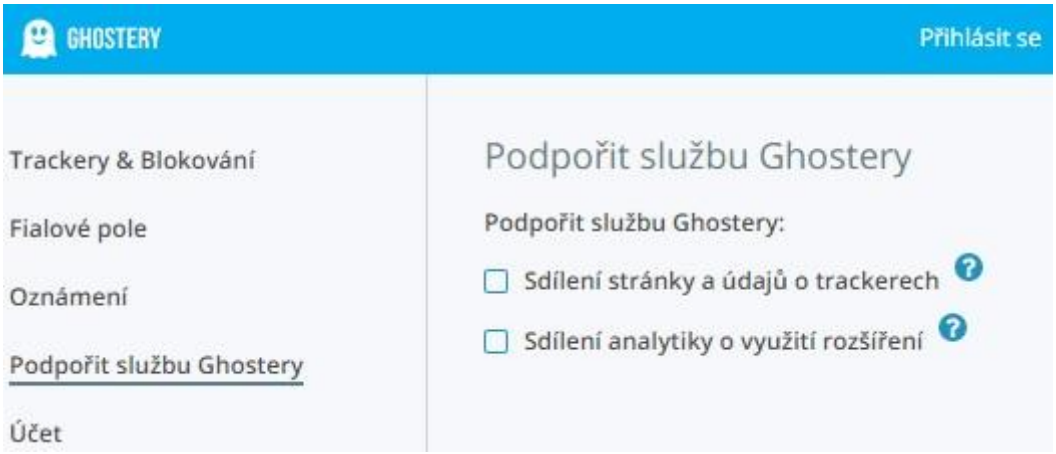
Obrázek představuje hlavní panel programu AdBlock s jeho nastavením.

Ghostery (dostupný pro Chrome, Firefox, Operu i Safari)



***Obr. 20**: Ghostery v Google Chrome (Zdroj: autor)*

Ghostery detekuje a blokuje sledovací technologie pro rychlejší načítání stránek a ochranu dat. Je možné zde nastavit trackery, které chce uživatel blokovat, jak po jednotlivých, tak podle kategorií. Jedná se o kategorie: reklama, webová analytika, interakce zákazníků, sociální média, základní, přehrávač audia/videa, reklama pro dospělé a komentáře. Dále je možné zde nastavit důvěryhodné weby, jejichž prohlížení nebude omezováno a všechny trackery na těchto stránkách nejsou pak blokovány. Také je možné nastavit nepřístupné weby. [69]



***Obr. 21**: Vypnutí zasílání osobních údajů v Ghostery v Google Chrome (Zdroj: autor)*

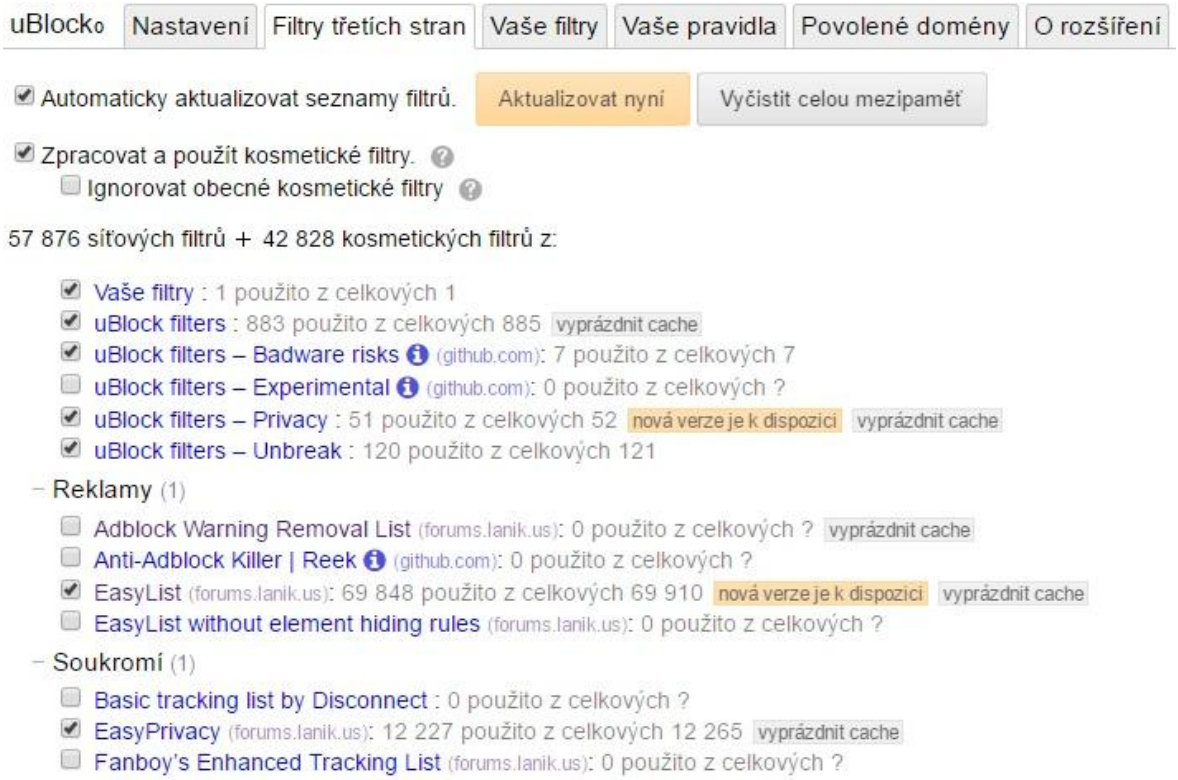
Obrázek znázorňuje vypnutí zasílání osobních údajů v Ghostery v Google Chrome. I v případě add onů je nutné si prověřit, zda neshromažďuje osobní údaje. Pokud je zapnuté sdílení stránky a údajů o trackerech a sdílení analytiky o využití rozšíření, zasílají se add onu Ghostery informace o aktivitách uživatele. Z tohoto důvodu nejsou tyto možnosti zaškrtnuté.

Ghostery byl vybrán z toho důvodu, že průměrné načtení stránky je rychlé, 3,6 sekund, málo zatěžuje paměť – zde nejrychlejší (37MB) a málo zatěžuje CPU na 6,4%.

uBlock Origin (dostupný pro Chrome, Firefox)

Byl vybrán z toho důvodu, že průměrná doba načtení stránky je 3,2 sekundy, je nejrychlejší, po Ghostery nejméně zatěžuje pamět (48MB) a nejméně zatěžuje CPU 4,6%.

Co je u tohoto ad blockeru zajímavé, že uBlock Origin umožňuje nastavení filtrů třetích stran.



***Obr. 22**: Seznam filtrů třetích stran v uBlock Origin v Google Chrome (Zdroj: autor)*

Obrázek ukazuje seznam filtrů třetích stran. Tento seznam filtrů, tzv. FilterList, poskytuje obsáhlou databázi, ze které si každý uživatel může vybrat své seznamy, nebo-li své vlastní nastavení ochrany soukromí. To znamená, že pokud je v reklamních filtrech zaškrtnutý EasyList, blokuje uBlock Origin reklamu z anglických stránek obsahující neočekávané snímky, obrázky a objekty. Tyto filtry je možné vzájemně kombinovat dle požadavků uživatele. UBlock Origin pak blokuje to, co si uživatel zvolil ve FilterListu. [70]

UBlock Origin obsahuje panel s dynamickým filtrováním. Ten obsahuje informace o tom, co je dynamicky filtrováno.

***Obr. 23**: Dynamické filtrování v uBlock Origin v Google Chrome (Zdroj: autor)*

Obrázek zobrazuje panel dynamického filtrování v uBlock Origin. V prvním sloupci je vidět co je možné dynamicky filtrovat. Ve druhém sloupci je možné nastavit globální pravidla dynamického filtrování, jakékoliv pravidlo se objeví zde v tomto sloupci je aplikováno všude, na všech stránkách. V tomto případě jsou filtrovány rámce třetích stran. Třetí sloupec obsahuje lokální pravidla dynamického filtrování, jakékoliv pravidlo objevící se v tomto sloupci, se vztahuje pouze na aktuální stránku. [71]

Přehled blokovaných/povolených požadavků

- nebo + = 1 – 9 síťových požadavků byly blokovány nebo povoleny,
-- nebo ++ = 10 – 99 síťových požadavků byly blokovány nebo povoleny,
--- nebo +++ = 100 nebo více síťových požadavků byly blokovány nebo povoleny,
prázdné bunky = nejsou nastaveny žádné síťové požadavky pro konkrétní hostname. [71]

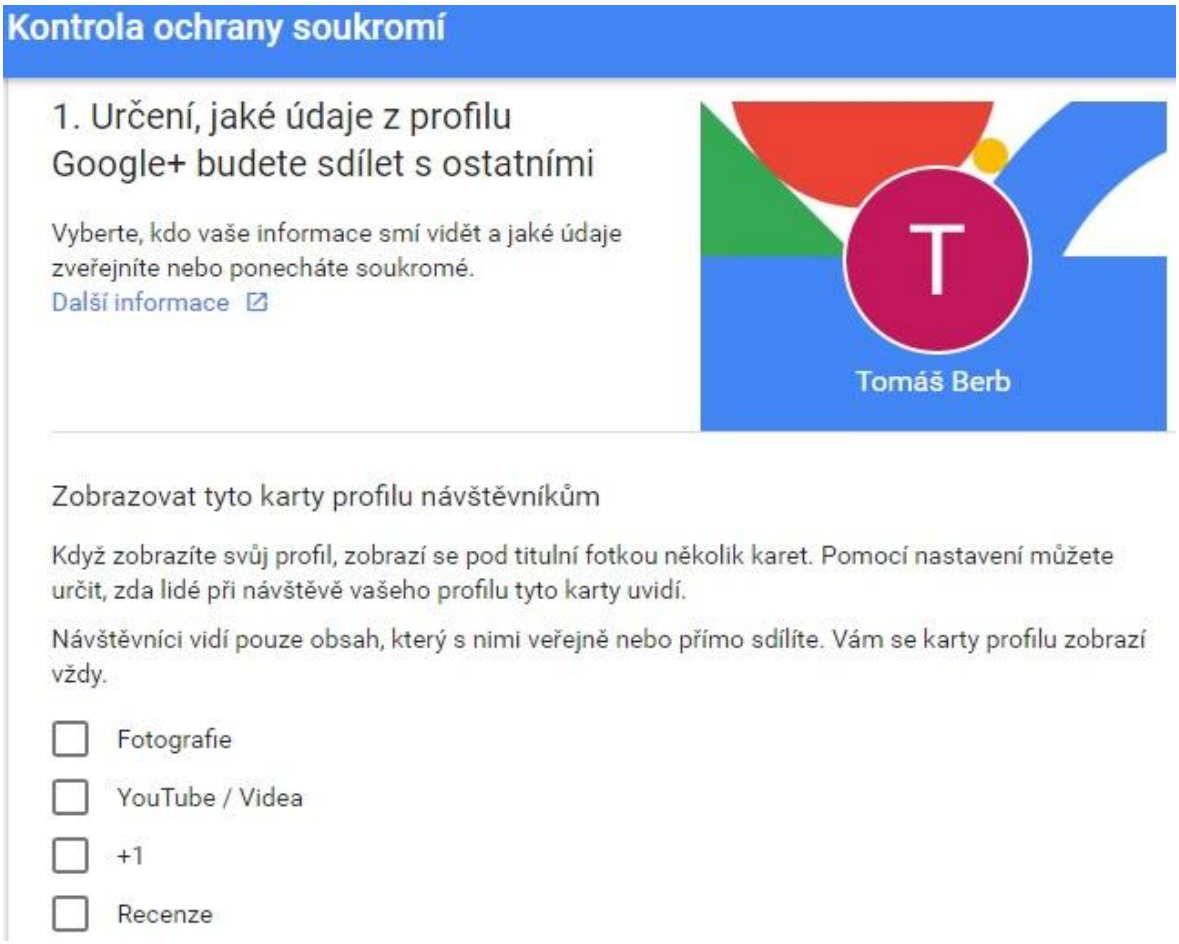
Statické filtrování se vztahuje na filtry, které pochází z FilterListu (EasyList, EasyPrivacy, hpHosts). Dynamické filtrování jsou pravidla filtrování, které mají nádech pravidel firewallu.

4.3.3 Google

V této podkapitole bude nastavena ochrana soukromí, ovládacích prvků aktivity a personalizace.

Ochrana soukromí

Při návštěvě uživatelského účtu v části Osobní údaje a ochrana soukromí se nastaví, jaké údaje mají být zveřejněny a jaké soukromé.

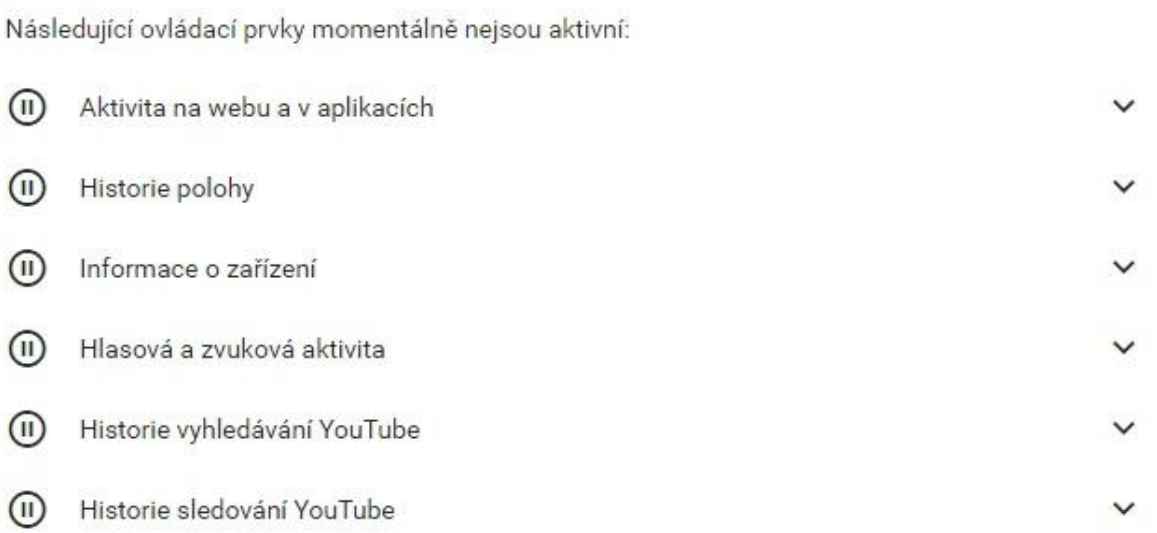


***Obr. 24**: Kontrola ochrany soukromí v Googlu (Zdroj: autor)*

Obrázek znázorňuje, jaké údaje z profilu Google+ jsou sdíleny s ostatními. V této části bylo vybráno, aby při zobrazení profilu nikdo neviděl tyto karty.

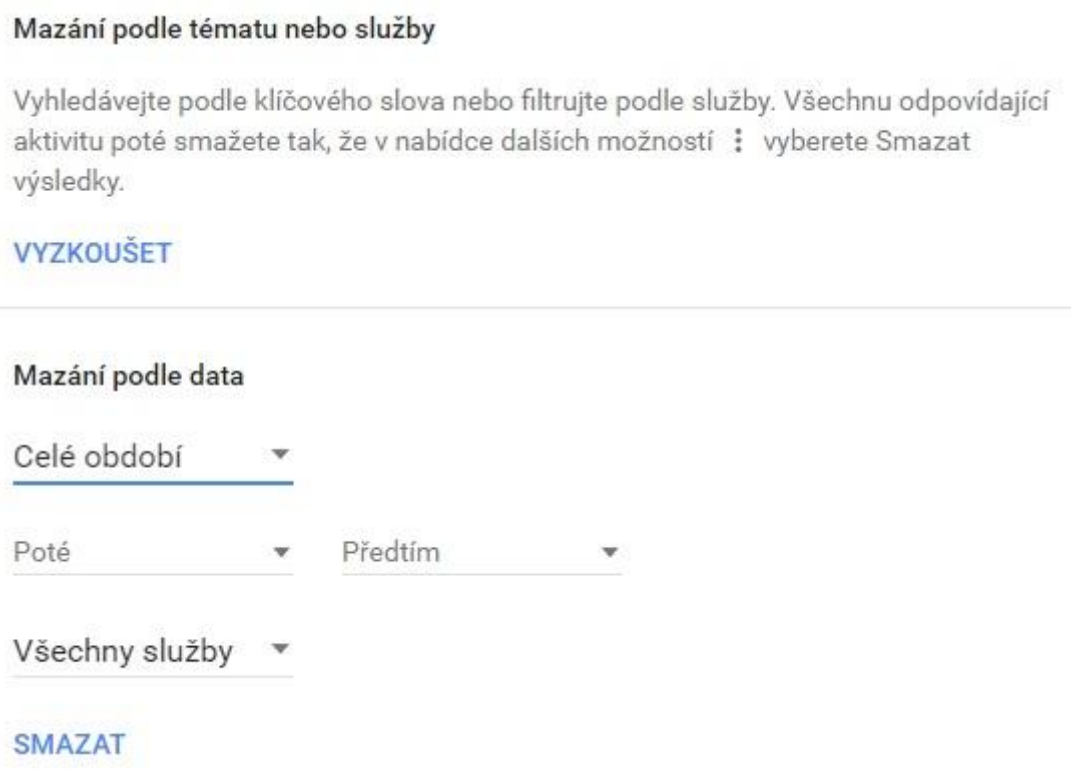
Konfigurace služeb Google

V této podkapitole se nachází konfigurace ovládacích prvků aktivity a mazání a vypnutí historie služeb.



***Obr. 25**: Nastavení ovládacích prvků aktivity na Googlu (Zdroj: autor)*

Obrázek ukazuje nastavení ovládacích prvků aktivity. Google ve svých službách ukládá údaje o aktivitě. Nejprve byla smazána historie aktivity na webu a v aplikacích pro celé období. Poté byla služba vypnuta. Stejně tak bylo učiněno s historií polohy, informacích o zařízení, hlasovou a zvukovou aktivitou, historií vyhledávání Youtube a historií sledování Youtube.



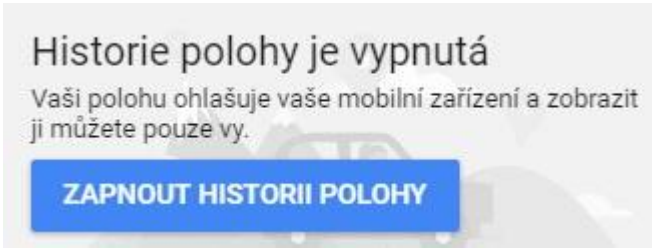
***Obr. 26**: Mazání podle tématu nebo služby v Googlu (Zdroj: autor)*

Obrázek ukazuje, jak byla vymazána aktivita na webu a aplikacích.

Podle časové osy je možné sledovat místa a trasy, které uživatel navštívil a po kterých cestoval. Historie polohy vytváří soukromou mapu míst, kde se uživatel pohybuje se zařízeními, ve kterých je přihlášen.

***Obr. 27**: Smazání historie polohy v Googlu (Zdroj: autor)*

Obrázek ukazuje smazání celé historie polohy.

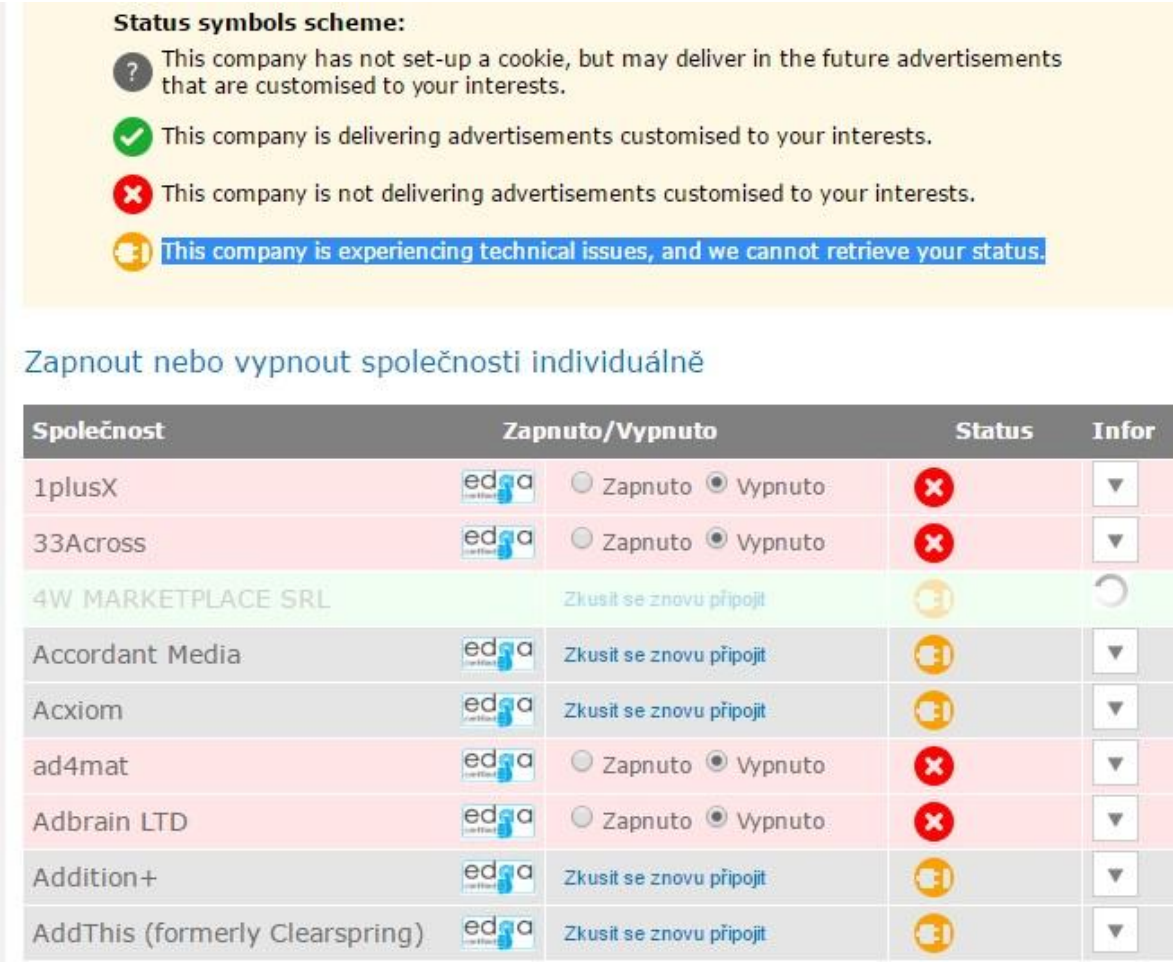


***Obr. 28**: Vypnutí historie polohy v Googlu (Zdroj: autor)*

Obrázek ukazuje vypnutí historie polohy.

Konfigurace personalizace

V případě konfigurace personalizace byl autor přesměrován na tuto stránku http://www.youronlinechoices.com/cz/vase-volby.



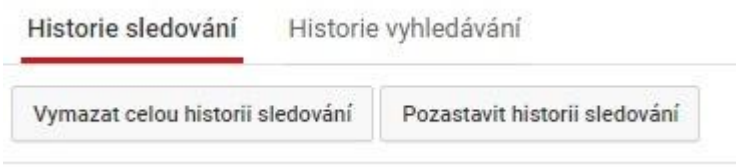
***Obr. 29**: Konfigurace personalizace v Googlu (Zdroj: autor)*

Obrázek ukazuje konfiguraci personalizace. Je zde vidět, jaké společnosti shromažďují a používají informace k poskytování online behaviorální reklamy. Autor zvolil požadavek vypnutí shromažďování údajů od všech společností třetích stran. Bohužel některé nebylo možné vypnout z toho důvodu, že se na ně dle této stránky nebylo možné v danou chvíli připojit. Připojení autor zkoušel vícekrát za týden.

Důležité je, že zde nejsou vypínány veškeré internetové reklamy, ale pouze reklamy, které jsou přizpůsobeny uživatelským zájmům založeným na předchozí aktivitě na webových stránkách.

4.3.4 Youtube

Sledování uživatelů v Youtube je možné vypnout přes uživatelský účet Google, aby nedocházelo k propojení mezi účty a dále také na domovské stránce Youtube.



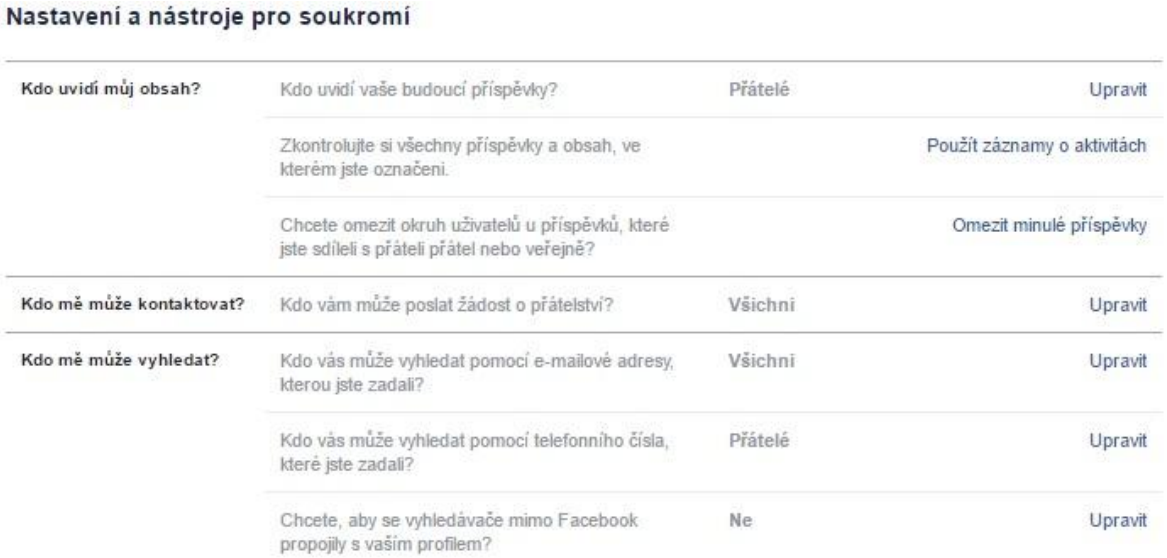
***Obr. 30**: Vymazání a pozastavení historie sledování na Youtube (Zdroj: autor)*

Na stránce Youtube je možné po přihlášení k uživatelskému účtu v nastavení zvolit políčko Historie, kde se dá nastavit historie sledování a historie vyhledávání. U historie sledování Autor nejprve vymazal celou historii sledování a poté pozastavil historii sledování, stejný proces provedl také u historie vyhledávání.

4.3.5 Facebook

V této podkapitole se nachází ochrana soukromí na sociální síti Facebook. Je zde představena ochrana uživatelského soukromí, nastavení ochrany označování a přidávání polohy. Pro tuto kapitolu autor čerpal ze zdroje [72].

Ochrana soukromí



***Obr. 31**: Nastavení a nástroje pro soukromí na Facebooku (Zdroj: autor)*

Z obrázku je vidět nastavení a nástroje pro soukromí. Uživatel může nastavit, kdo uvidí jeho budoucí příspěvky. Sdílet příspěvky je možné pouze mezi přáteli Facebooku a nebo další alternativou je sdílet příspěvky pouze mezi blízkými přáteli, kde si uživatel sám

může definovat okruh těchto lidí. Dále je možné zvolit, kdo může uživatele vyhledat pomocí e-mailové adresy nebo telefonního čísla.

Další důležitou funkcí je nastavení, zda uživatel chce, aby se vyhledávače mimo Facebook propojily s uživatelským profilem. Zde je nastaveno ne z toho důvodu, aby se vyhledávače mimo Facebook nepropojily s profilem.

Zobrazování online reklam založených na zájmech Facebookem a dalších zapojených společností je možné odmítnout prostřednictvím stejné webové stránky jako v kapitole 08.

Nastavení ochrany označování

V této podkapitole je provedeno nastavení ochrany označování.

***Obr. 32**: Nastavení Timeline a označování na Facebooku (Zdroj: autor)*

Obrázek ukazuje nastavení Timeline a označování na Facebooku. V této sekci může uživatel v rámci ochrany soukromí definovat:

- kdo může přidávat příspěvek na jeho Timeline,
- kontrola příspěvků, v nichž ho přátelé označí, než se objeví na jeho Timeline,
- co ostatní vidí na jeho Timeline,

- kdo vidí příspěvky, na kterých je na své Timeline označen,
- kdo uvidí příspěvky, které na jeho Timeline přidávají druzí,
- pokud je uživatel označen v příspěvku, kdo může označení uživatele vidět,
- kontrola označení, která lidé přidají k jeho příspěvkům, než se označení objeví na Facebooku.

***Obr. 33**: Záznamy o aktivitách na Facebooku (Zdroj: autor)*

Z Facebooku se dají odstranit záznamy o aktivitách v Záznamy o aktivitách. Není ale možné je odstranit globálně, ale pouze určité příspěvky po jednom.

Přidání polohy - Geotagging

Pokud uživatel nechce, aby Facebook dostával a prezentoval informace o poloze, kde se nachází, je možné toto nastavení vypnout. Získávání údajů o poloze je třeba nejprve zakázat na mobilních telefonech nebo zařízení. Při první instalaci Facebooku na mobilní zařízení většinou žádá o povolení k použití lokalizačních služeb telefonu tak, aby mohl poskytnout možnost „check-in“ na různých místech a tagovat fotografie s lokačními informacemi. V případě, že uživatel nechce, aby Facebook věděl, z jakých míst na něj fotografie vkládáme, pak by měšl odvolat toto oprávnění v nastavení lokačních služeb telefonu.

Jak bylo již zmíněno na obrázku 34, je možné selektivně zabránit lidem uživatele tagovat. Jedná se o nastavení: Jak můžu spravovat označení, která lidé přidají a návrhy na označení? V případě zapnutí funkce umožňuje uživateli přezkoumat vše kde byl označen, ať už je to obrázek nebo lokační check-in. Je možné rozhodnout, zda tag bude zveřejněn dříve než je umístěn na internet.

Odstranění Geotagů z obrázků předtím než jsou umístěny na Facebook

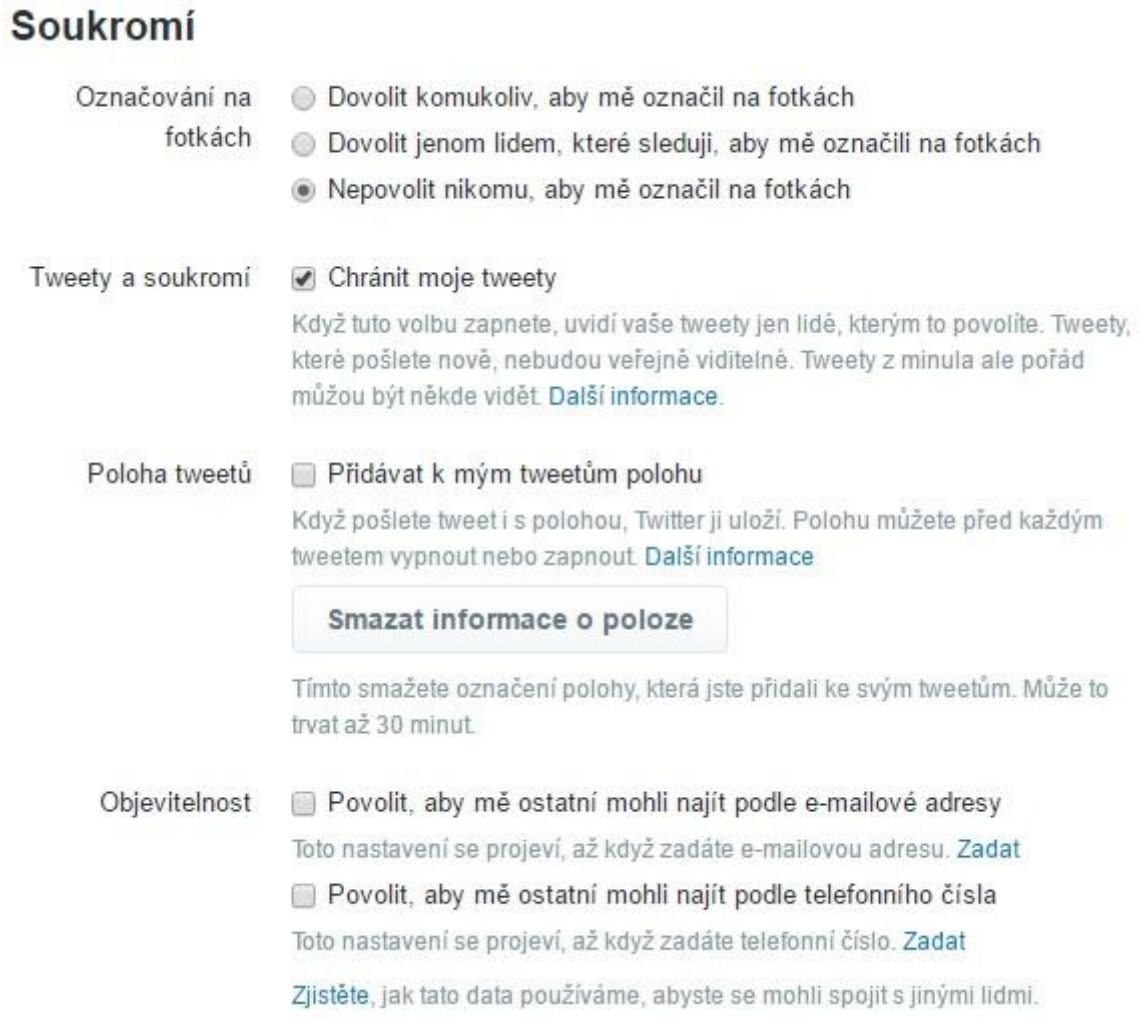
Pro zajištění, že obrázky poslané na Facebook a další sociální sítě neodhalují informace o aktuální poloze, musí se uživatel ujistit, že informace o geotagu nejsou

zaznamenávány. Většinou je to provedeno vypnutím lokalizační služby na mobilním a jiném zařízení, takže se informace o geotagu nenahrávají do obrázkových Exif metadat. Existují také aplikace, které umožňují se zbavit lokačních informacích u souborů, které již uživatel pořídil.

Pro iPhone je to deGeo a nebo Photo Editor Privacy pro Android k odstranění informací zeměpisných souřadnicích z vašich fotografií před nahráním na sociální média.

Twitter

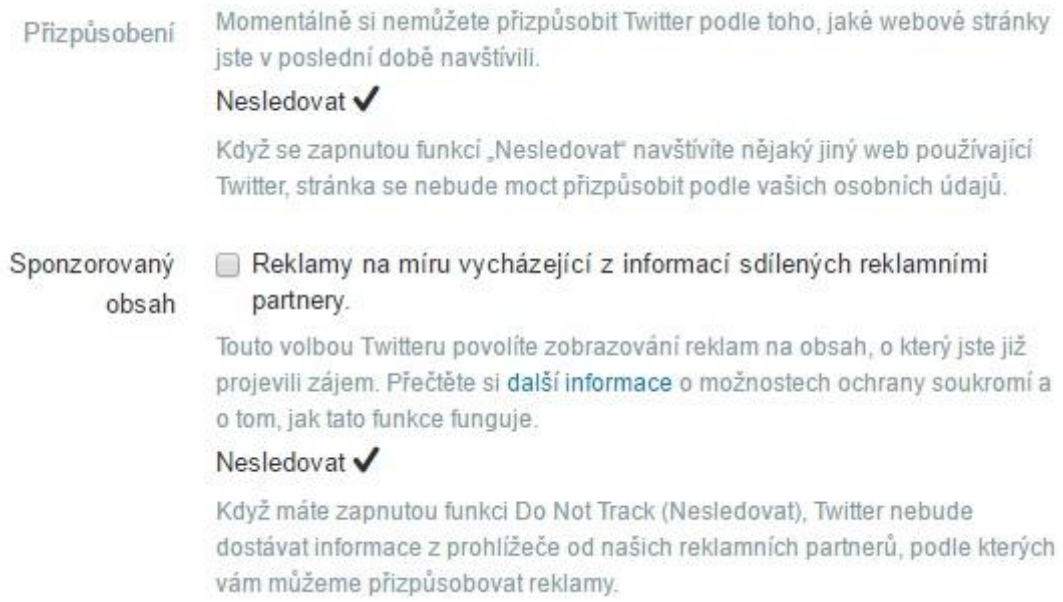
Tato podkapitola se věnuje nastavení ochrany soukromí na Twitteru.



***Obr. 35**: Nastavení soukromí na Twitteru (Zdroj: autor)*

Obrázek ukazuje nastavení soukromí na Twitteru. Autor nepovolil nikomu, aby ho označoval na fotkách, jeho Tweety uvidí pouze lidé, kterým to povolí, nebudou tak veřejně viditelné. Je zde možné smazat Tweety z minulé doby. Dále není dovoleno přidávat ke

Tweetům polohu, takže není vidět, kde byl Tweet přidán, uživatelé nemohou autora vyhledat pomocí e-mailové adresy, ani telefonního čísla.



***Obr. 36**: Nastavení přizpůsobení osobních údajů na Twitteru (Zdroj: autor)*

Obrázek ukazuje nastavení přizpůsobení osobních údajů podle potřeb autora, kde je nastaveno nesledovat z toho důvodu, aby se obsah nepřizpůsoboval podle jeho osobních údajů. Reklamy se také nebudou zobrazovat tak zvaně na míru autora, autor má dále zapnutou funkci Do Not Track.

Instagram

Tato podkapitola zobrazuje ochranu soukromí na Instagramu.

***Obr. 37**: Nastavení soukromého účtu na Instagramu (Zdroj: autor)*

Obrázek znázorňuje nastavení soukromého účtu na Instagramu. Pokud je účet nastavený jako soukromý, nemohou uživatelé, kterým autor neschválil žádost sledování veřejně sledovat jeho profil. Autorův profil je tak viditelný pouze uživatelům, kterým schválil požadavek sledování a není možné fotky vyhledat ani ve webových

vyhledávačích. Jeho fotografie nejsou také viditelné i v případě, že je k jeho fotce přidán komentář s hashtagem.

4.4 Reaktivnípřístup obrany

Cílem této kapitoly je v rámci reaktivního přístupu obrany zpracovat případovou studii k minimalizování nebo úplné eliminaci výskytu osobních údajů autora z výsledku vybraného internetového vyhledávače. V první řadě je provedena analýza výskytu stop o autorovi z výsledků vyhledávání Google a následně pokus o odstranění výskytu stop o autorovi z výsledků vyhledávání Google.

4.4.1 Analýza výskytu stop o autorovi z výsledků vyhledávání Google

V první řadě je třeba říct, že odstranění informací z výsledků vyhledávání Google neznamená, že jsou informace odstraněny z celého internetu. Odstranění informací z výsledků vyhledávání Google znamená pouze odstranění z výsledků vyhledávání tohoto vyhledávače. Pokud chce uživatel odstranit informace z internetu, je nutné informace smazat ze zdrojové stránky. Pro odstranění konkrétní informace/stopy z celého internetu je nutné znát zdroj obsahu a jeho vlastníka.

V první řadě autor zadal své jméno do vyhledávače Google.

***Obr. 38**: Digitální stopa o autorovi ve vyhledávači Google (Zdroj: autor)*

Obrázek ukazuje, že ve výsledku vyhledávače Google je pouze jedna stopa o autorovi, jedná se o profil Facebooku.

Autor také zkusil zobrazit obrázky při vyhledávání svého jména.

***Obr. 39**: Digitální stopa o autorovi v obrázcích ve vyhledávači Google (Zdroj: autor)*

Obrázek znázornuje, že o autorovi jsou ve výsledku vyhledávače Google v sekci obrázky umístěny tři obrázky, které odkazují na webovou stránku http://www.hara-gym.cz/?p=1275.

4.4.2 Odstranění výskytu stop o autorovi z výsledků vyhledávání Google

Pro skrytí obsahu, nebo-li odstranění z výsledků vyhledávání Google, je nutné zablokovat nebo odstranit všechny varianty adresy URL dotyčného obsahu, protože různé adresy URL mnohokrát odkazují na stejný obsah.

Digitální stopu ze stránky Facebook autor odstranil pomocí nastavení v ochraně soukromí na této sociální síti viz kapitola 05

Autor chce dále z vyhledávače Google odstranit 3 fotografie, které odkazují na stránku Hara Gymu. Google ale ve svých zásadách uvádí, že v první řadě je nutné zažádat vlastníka stránky, aby stopy o uživateli z internetu odstranil. V případě, že jsou informaci o uživateli odstraněny z příslušné stránky, ale dále se autor vyskytuje ve výsledcích vyhledávání Google, jedná se o odstranění stop z mezipaměti. V tomto případě je možné informace o uživateli z mezipaměti odstranit. [73] [74]

Informace, které Google může odstranit

- Národní identifikační čísla, jako je číslo sociálního zabezpečení ve Spojených státech, číslo daňového poplatníka v Argentině, Cadastro de pessoas Físicas v Brazílii, registrační číslo občana v Koreji, identifikační karta občana v Číně apod.,
- čísla bankovních účtů,
- čísla platebních karet,
- obrázky podpisů,

- záznamy, kde jste zachyceni nazí nebo v sexuálně explicitním kontextu a které byly nahrány nebo sdíleny bez vašeho vědomí. [74]

Informace, které Google obvykle neodstraňuje

- Datum narození,
- adresy,
- telefonní čísla. [74]

Dle informací které Google může odstranit je vidět, že tyto informace musí být odstraněny na zdrojové stránce a poté z výsledků vyhledávání Googlu, jinak Google autorovi nebude nápomocen.

Autor diplomové práce tedy zažádal vlastníka stránky Hara Gymu emailem o odstranění fotografií. Vlastník stránek Hara Gymu ale na výzvy k odstranění fotografií nereagoval, a tak se autor obrátil na ÚOOÚ.

ÚOOÚ autorovi sdělil, že se tato záležitost řeší dle § 84 Nový občanský zákoník č. 89/2012 Sb. V tomto paragrafuje je řečeno, že zachytit jakýmkoli způsobem podobu člověka tak, aby se podle zobrazení dala určit jeho totožnost je možné pouze s jeho svolením. V případě, že vlastník stránek nereaguje, je nutné se obrátit na soud, který rozhodne, zda mají být fotografie staženy či ne. Pokud soud rozhodne ve prospěch autora diplomové práce, bude muset webová stránka fotografie smazat. V případě, že i nadále se budou fotografie zobrazovat ve vyhledávači Google, má se autor obrátit na ÚOOÚ, který bude žádost o smazání z vyhledávání řešit. [75]

5 Výsledky a diskuse

V této kapitole je provedeno zhodnocení výsledků a diskuze.

Hlavním cílem diplomové práce bylo analyzovat typy osobních údajů dostupných z internetu a vytvořit systematické shrnutí nástrojů a metod pro tvorbu ochrany soukromí uživatelů v internetu.

Praktická část se zabývala vytvořením souhrnu identifikací online signálů, které jsou získávány a sledovány o uživatelích internetu. Na základě výsledků ze souhrnu byl vytvořen proaktivní a reaktivní přístup obrany proti zneužívání osobních a citlivých údajů v internetu.

5.1 Výsledky

5.1.1 Souhrn celkového množství nalezených signálů

Pro tvorbu souhrnu celkového množství nalezených signálů autor použil doplněk Lightbeam, cookies v historii prohlížeče, dále Panopticlick, Clickclickclick.click, BrowserLeaks a také informace na stránkách Google, Youtube, Facebook, Instagram a Twitter.

Lightbeam

V doplňku Firefoxu Lightbeam se podařilo ukázat, jak jsou webové stránky mezi sebou vzájemně propojeny pomocí cookies třetích stran. Dle výsledků testování s přibývajícími požadavky operací počet cookies třetích stran narůstal. Test se prováděl pro stránky Facebook, Google, Seznam a Youtube, kde byly stránky nejprve otevřeny a následně se autor přihlásil do uživatelských účtů a zadal jeden požadavek na každé stránce. V porovnání s pouze navštívenými 4 vybranými stránkami, kde počet cookies třetích stran činil 21, vzrostl počet cookies třetích stran po přihlášení na stránky a zadání jednoho požadavku na každé stránce o více jak 42%.

Cookies v historii prohlížeče

V této části bylo ukázáno, jaké množství cookies je nahráváno do prohlížeče Mozilla Firefox. Po otevření stránek Google.cz, Youtube.com, Facebook.com a Seznam.cz se do prohlížeče Mozilla Firefox nahraje 50 cookies z 18 serverů. Pokud se autor přihlásil dále do uživatelských účtů těchto stránek, do prohlížeče se nahrálo celkem 87 cookies.

Panopticlick

Projekt Panopticlick představil, jak je možné ověřit nastavení zabezpečení v prohlížeči Google Chrome. Zajímavé bylo, že stejný otisk prohlížeče jako autorův sdílí jeden ze 164 799 testovaných prohlížečů a přesnost stránky Panopticlick odhadnout otisk prohlížeče je 83,6%.

Clickclickclick.click

Tato webová stránka představila, jak je sledován každý pohyb uživatele na internetu. Sleduje detaily akcí v reálném čase a ukazuje to jak v písemné, tak vokální podobě. Dá se předpokládat, že na základě působení uživatele na webových stránkách dokáže odhadnout psychologii člověka.

BrowserLeaks

BrowserLeaks znázornila, že že je možné sledovat jak IP adresu, informace o JavaScriptu prohlížeče, ale také HTML5 Geolokaci a otisk prohlížeče. Tato stránka identifikovala autorovu přesnou adresu bydliště. Dále mu sdělila, že ze 160 175 User-Agentů má 3830 stejný otisk jako autor, což činí 2,39%.

Google, Youtube, Facebook, Instagram, Twitter

Na těchto webových stránkách autor zjišťoval, jaké informace o uživatelích shromažďují. Tyto stránky si autor zvolil z toho důvodu, že jsou to jedny z nejnavštěvovanějších stránek u nás i ve světě.

Na základě shromažďování dat z uvedených nástojů a stránek se podařil vyhotovit souhrn celkového množství nalezených signálů, které je možné o uživatelích sledovat. Signály byly rozděleny do dvou hlavních skupin: údaje o uživateli a údaje o zařízení. Údaje o uživateli byly dále rozděleny na osobní údaje, interakce s webovou stránkou a informace o poloze. Údaje o zařízení obsahovaly informace z protokolu mobilního telefonu a technické údaje. V každé podskupině se nacházely konkrétní údaje.

5.1.2 Proaktivní přístup obrany

V proaktivním přístupu obrany byla provedena konfigurace ochrany soukromí webového prohlížeče Google Chrome. Následně byly vybrány programy pro ochranu

osobních údajů. Jednalo se o AdBlock, Ghostery a uBlock Origin. Poté byla nastavena ochrana soukromí na vybraných webových stránkách jako Google, Youtube, Facebook, Twitter a Instagram.

5.1.3 Reaktivní přístup obrany

V reaktivním přístupu obrany byla vytvořena případová studie k minimalizování nebo úplné eliminaci výskytu osobních údajů autora z výsledku vybraného internetového vyhledávače. Uživatel má právo na smazání fotografií, na kterých se nachází na webových stránkách. Pokud se fotografie nachází ve vyhledávači Google, musí být fotografie nejprve smazána ze zdrojové stránky. V případě ale odmítnutí webové stránky smazat fotografie s jeho osobou, je třeba podstoupit další kroky a dát tuto záležitost k soudu. Soud následně rozhodne buď ve prospěch osoby na fotografii nebo ve prospěch webové stránky.

5.2 Diskuse

Při psaní této diplomové práce mě překvapilo, co vše je možné o uživatelích internetu zjistit. Světové korporace mohou sledovat nejen osobní údaje, technické údaje o softwaru, hardwaru, mohou také sledovat polohu uživatele a na základě jeho interakce s webovou stránkou odhadnout jeho psychologii. Tyto korporace tedy ví, kde bydlím, jaké mám technické zařízení, jaký software a doplňky používám, co vyhledávám a jak na stránky reaguji. Vědí o člověku mnohem více informací než kdokoliv jiný. Je ale otázkou, zda se tyto údaje opravdu používají anonymně nebo mají možnost je vázat k určité osobě. ÚOOÚ se ale s porušováním těchto práv v posledních letech nesetkal.

V rámci proaktivního přístupu obrany může člověk nastavit svoji ochranu soukromí na internetu. I když takto část dle mého názoru není také jednoduchá, uživatel musí prohlížeč a webové stránky pro obranu nastavit, musí konfiguraci kontrolovat, mazat historii prohlížeče a potažmo si musí dát pozor, jaké webové stránky navštěvuje. Proaktivní přístup je ale stále možností volby uživatele, jak si obranu nastaví a jaké stránky navštíví.

Větší problém vidím u reaktivního přístupu obrany. Zde byl ukázán problém se smazáním fotografií autora z výsledků vyhledávání. Jak jednou uživatel dá možnost informace o jeho osobě na internetu zveřejnit, je velmi zdlouhavé a časově náročné docílit svých práv. Z tohoto důvodu bych daleko větší důraz kladl na informace, které o sobě uživatel zveřejňuje na sociálních sítích nebo webových stránkách, protože tyto údaje jsou

takřka neodstranitelné. Každý by měl mít právo, aby informace o něm byly odstraněny za jakýchkoliv podmínek, a to transparentně a rychle.

Závěr

Nacházíme se v době internetu a sociálních sítí. Internet se stal hlavním nástrojem používaným pro komunikaci mezi celým světem. Není to jen místo, které nám poskytuje informace, ale místo kde si člověk utváří svoji identitu stejně jako v práci, ve škole nebo na hřišti s kamarády. Na internetu uživatel zanechává stopy, které celosvětové korporace dokážou shromažďovat a dohledat téměř vše co člověk sdílí a potažmo jak se na internetu pohybuje. Je tak velmi složité udržet si v tomto virtuálním světě soukromí nebo anonymitu.

V této diplomové práci byl řešen problém ochrany soukromí uživatelů v internetu. Teoretická část byla zaměřena na analýzu způsobů sledování a shromažďování osobních údajů o uživatelích na internetu prostřednictvím vhodných technologií a na shrnutí nejčastějších důvodů a dopadů sledování osobních údajů na internetu. V praktické části byla provedena identifikace online signálů, které jsou získávány a sledovány o uživatelích internetu, byl zpracován souhrn identifikovaných online signálů a vytvořen soubor doporučení proaktivního a reaktivního přístupu obrany proti zneužívání osobních a citlivých údajů v internetu.

Teoretická část se zabývala osobními a citlivými údaji, pro pochopení obsáhlosti vybraného tématu byla uvedena současná situace užívání internetu ve světě a ČR a vybrány sledovací nástroje pro následnou analýzu, jaká data jsou o uživatelích internetu sledována a shromažďována. Jedná se o webové stránky Google, Youtube, Facebook, Instagram a Twitter, zmíněny jsou také důvody výběru těchto nástrojů.

Dále byla provedena analýze způsobů sledování a shromažďování osobních údajů o uživatelích na internetu prostřednictvím vhodných nástrojů. Byly představeny sledovací technologie jako cookies, webové štěnice, etag, zombie cookies, evercookies, pluginy sociálních sítí, web storage, canvas fingerprinting a akcelerometr a vysvětleny jejich principy fungování.

Následně byly uvedeny důvody a dopady shromažďování osobních a citlivých údajů. Tato část se zabývala personalizací, behaviorálním marketingem a profilováním uživatelů. Pro pochopení fungování behaviorálního marketingu byla ukázána Facebook analýzu ve Wolfram Alpha. Pro zjištění důvodů sledování údajů o uživatelích byly

vybrány stránky Google a Facebook. Kromě zřejmých dopadů, jakožto sledování a shromažďování osobních údajů, byl zvolen filter bubble.

V praktické části byly pro zjištění, jaké údaje jsou o uživatelích sledovány, použity Lightbeam, cookies v historii prohlížeče, Panopticlick, Clickclickclick.click, BrowserLeaks a vybrané webové stránky Google, Youtube, Facebook, Instagram a Twitter. Všechny tyto údaje byly pro každý nástroj a webovou stránku zdokumentovány.

Podle výsledků z vybraných stránek byla vyhotovena tabulka se souhrnem celkového množství nalezených signálů, které jsou o uživatelích internetu sledovány a shromažďovány. Souhrn byl rozdělen do jednotlivých kategorií dle druhu signálu.

V další části byl na základě výsledků ze souhrnu nalezených signálů vytvořen proaktivní a reaktivní přístup obrany proti zneužívání osobních a citlivých údajů v internetu.

V proaktivním přístupu obrany byly připraveny doporučení pro uchování anonymity uživatele v online prostředí. Ve webovém prohlížeči Google Chrome byla provedena konfigurace ochrany soukromí, souborů cookies, nastavení obsahu a byly smazány údaje o prohlížení. Následně byly vybrány 3 programy pro ukázku nastavení ochrany uživatele v internetu a uvedeny důvody výběru. Jedná se o AdBlock, Ghostery a uBlock Origin. Dále bylo provedeno nastavení proaktivního přístupu na webových stránkách Google, Youtube, Facebook, Twitter a Instagram.

V uživatelském účtu Googlu byla provedena konfigurace ochrany soukromí, služeb Google a personalizace. U ochrany soukromí se jednalo o nastavení jaké údaje z profilu Google+ jsou sdíleny s ostatními, u ovládacích prvků aktivity o smazání historie aktivity na webu a v aplikacích pro celé období a následně o vypnutí této služby a smazání a vypnutí historie polohy. V konfiguraci personalizace bylo zažádáno o vypnutí shromaždování údajů od všech společností třetích stran. Ačkoliv bylo v Youtube vypnuto sledování přes uživatelský účet Google+, tato služba byla také vypnuta na domovské stránce Youtube.

Ve Facebooku byla nastavena ochrana soukromí, označování a přidávání polohy. Konfigurace ochrany soukromí byla nastavena také na Twitteru a Instagramu.

V reaktivním přístupu obrany byla vytvořena případová studie zabývající se minimalizováním nebo úplnou eliminací výskytu osobních údajů autora z výsledku vyhledávání internetového vyhledávače Google.

Ve vyhledávači Google byly o autorovi nalezeny digitálni stopy ze stránek Facebook a Hara Gym. Facebookový profil se z vyhledávače Google odstranit podařilo. Nepodařilo se ale odstranit údaje ze stránky Hara Gym. Na žádost zaslanou emailem autor nedostal žádnou odpověď a tak webová stránka brání autorovi ve smazání fotografií. Po obrácení se v této záležitosti na ÚOOÚ bylo autorovi sděleno, že mám právo na smazání fotografií, na kterých se nachází na stránce Hara Gymu. V případě ale odmítnutí webové stránky smazat fotografie s jeho osobou, je třeba podstoupit další kroky a dát tuto záležitost k soudu. Soud následně rozhodne buď ve prospěch autora, nebo ve prospěch webové stránky. Tuto fázi ale autor ve své diplomové práci nepodstoupil.

Soukromí v internetu hraje pro člověka v dnešním světě důležitou roli a snaží se ho co nejlépe chránit. Informace o každém z nás jsou na internetu velmi cenné a firmy zpracovávající osobní údaje častokrát znají lidskou osobnost lépe než kdokoliv jiný.

Je ale možné, že se člověk stává více anonymní tím, že si své soukromí na internetu pomocí proaktivního přístupu nebrání. Čím více je prováděna konfigurace doplňků pro zvýšení anonymity, tím více se člověk liší od běžných uživatelů a jeho otisk má vyšší procento jedinečnosti. Je možné pro každou žádost používat anonymní okno nebo zakázat ukládání do mezipaměti, ale to není komfortní způsob pro běžného uživatele jak se pohybovat na internetu.

Dle této diplomové práce může uživatel konfigurovat svůj webový prohlížeč, vyhledávač Google, Facebook, Youtube, Instagram a Twitter a jsou mu doporučeny programy proti sledování třetích stran. Poté už musí sám uživatel vybírat, jaké webové stránky navštěvuje a snažit se navštěhovat pouze ty ověřené. Tak je vysoká pravděpodobnost, že si zachová v rámci proaktivního přístupu anonymitu na internetu.

Terminologický slovník

Tabulka 5: *Terminologický slovník (Zdroj: autor)*

Termín	Zkratka	Význam [zdroj]
Hypertext Transfer Protocol	HTTP protokol	HTTP protokol používá port 80 pro komunikaci mezi klientským zařízením a serverem. Výměna dat se provádí pomocí relací. HTTP relace je sekvence transakcí/přenosů. Tyto přenosy se používají převážně k získání data z webového serveru (ve formě žádosti, klient dá požadavek) a následně k vrácení souborů/dat potřebných k zobrazení webové stránky ve webovém prohlížeči. Na konci relace je spojení uzavřeno. HTTP protokol je protokol bezstavový z toho důvodu, že si nepamatuje stav z jedné relace ke druhé. [22] [76]
Hypertext Transfer Protocol Secure	HTTPS protocol	Používá protokol HTTP, ale poskytuje navíc ochranu přenášených dat pomocí protokolů Secure Sockets Layer (SSL) a Transport Layer Security (TLS), které provádí šifrování a dešifrování dat. [22]
Cross-site Request Forgery	CSRF	Metoda útoku do internetových aplikací, většinou slouží k získání přístupu do aplikace. [77]
Cross-site scripting	XSS	Metoda narušení WWW stránek, která využívá bezpečnostní chyby ve skriptech. Slouží například k získání citlivých údajů o návštěvnících stránek. [77]
Document object model	DOM	Objektově orientovaná reprezentace HTML nebo XML dokumentu. [78]
Web Graphics Library	WebGL	WebGL je rozhraní JavaScriptu pro vykreslení interaktivní 3D grafiky pomocí kompatibilního webového prohlížeče bez nutnosti užití plug-inů. [79]
Jedinečný identifikátor zařízení	UUID	Jedinečný identifikátor zařízení je řetězec znaků, který do zařízení zakódoval výrobce a slouží k jednoznačné identifikaci zařízení (například číslo IMEI mobilního telefonu). [80]
Exchangeable image file format metadata	Exif	Specifikace pro formát metadat, který je vkládán do souborů digitálními fotoaparáty. [81]
Hashovací funkce	Hash	Matematická funkce pro převod vstupních dat do malého čísla, výstupem hashovací funkce je například otisk nebo fingerprint. [82]
DOM localStorage		Ukládá data bez žádného data expirace. [83]

Termín	Zkratka	Význam [zdroj]
DOM sessionStorage		Ukládá data pro jednu relaci. [83]
User Agent		Hlavička, kterou posílají prohlížeče pro svou identifikaci. [84]
Web Real-Time Communication	WebRTC	Tato technologie je založena na HTML 5 a dokáže nabídnout hlasový chat nebo videochat integrovaný přímo v internetovém prohlížeči. [85]
JavaScript		Objektově orientovaný programovací jazyk. [86] [87]

Zdroje

[1] Úřad. In: *Úřad pro ochranu osobních údajů* [online]. Praha, ©2013 [cit. 2017-03-25]. Dostupné z: https://www.uoou.cz/urad/ds-1059/p1=1059

[2] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016 [online]. Praha: *Úřad pro ochranu osobních údajů*, ©2013 [cit. 2017-03-12]. Dostupné z: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-6-rijna-2016/ds-3109/p1=3109

[3] POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer Press, 2007. Právo a IT. ISBN 978-80-251-1777-4.

[4] Zásady ochrany osobních údajů. *Google* [online]. Mountain View, Kalifornie, USA, ©2017 [cit. 2017-01-15]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/

[5] ZUIDERVEEN BORGESIUS, Frederik J. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review*. 2016, 32(2), 256-271. DOI: http://dx.doi.org/10.1016/j.clsr.2015.12.013. ISSN 02673649. Dostupné také z: http://www.sciencedirect.com/science/article/pii/S0267364915001788

[6] Daily time spent on social networking by internet users worldwide from 2012 to 2016 (in minutes). In: *Statistica* [online]. Johannes-Brahms-Platz 1, 20355 Hamburg, Germany: Ipsos Media, 2016 [cit. 2017-02-05]. Dostupné z: https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/

[7] WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2016 - Update. In: *Internet World Stats* [online]. Miniwatts Marketing Group, 2016 [cit. 2017-02-05]. Dostupné z: http://www.internetworldstats.com/stats.htm

[8] KOLÁŘ, Petr. Trendy v návštěvnosti internetu. In: *NetMonitor* [online]. Korunní 483/89, Praha 3 130 00: SPIR, 2016 [cit. 2017-02-05]. Dostupné z: http://www.netmonitor.cz/sites/default/files/prilohy/IAC%202016%20-%20NetMonitor%20ro%C4%8Denka%202015.pdf

[9] SMITH, Craig. 100 Amazing Google Search Statistics and Fun Facts (November 2016). In: *Formerly Digital Marketing Ramblings* [online]. 2017 [cit. 2017-02-23]. Dostupné z: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/

[10] YouTube Company Statistics. In: *Statistic Brain Research Institute* [online]. Los Angeles, 2016 [cit. 2017-02-23]. Dostupné z: http://www.statisticbrain.com/youtube-statistics/

[11] Desktop Search Engine Market Share. In: *Netmarketshare* [online]. ©2006-2017 [cit. 2017-02-05]. Dostupné z: https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0

[12] Share of desktop search traffic originating from Google in selected countries as of October 2016. In: *Statistica* [online]. ©2006-2017 [cit. 2017-02-05]. Dostupné z: https://www.statista.com/statistics/220534/googles-share-of-search-market-in-selected-countries/

[13] TOPlist - Historie. In: *TOPlist* [online]. nám. Dr. Václava Holého 1054/13, 180 00 Praha 8, (c)1997-2017 [cit. 2017-03-22]. Dostupné z: https://www.toplist.cz/stat/?a=history&type=4

[14] Most popular multi-platform web properties in the United States in November 2016, based on number of unique visitors (in millions). In: *Statistica* [online]. [cit. 2017-02-05]. Dostupné z: https://www.statista.com/statistics/271412/most-visited-us-web-properties-based-on-number-of-visitors/

[15] NOVOTNÝ, Michal. SOCIÁLNÍ SÍTĚ 2015: FACEBOOK VERSUS OSTATNÍ. In: *Markomu* [online]. 2015 [cit. 2017-02-05]. Dostupné z: https://www.markomu.cz/socialni-site-2015/

[16] SMITH, Kit. Marketing: 47 Facebook Statistics for 2016. In: *Brandwatch* [online]. 1st Floor, Sovereign House, Church Street, Brighton, BN1 1UJ: Smith, 2016 [cit. 2017-02-05]. Dostupné z: https://www.brandwatch.com/blog/47-facebook-statistics-2016/

[17] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. Právo a IT. ISBN 978-80-247-5595-3.

[18] Share of U.S. population who have used YouTube to watch music videos or listen to music as of February 2016, by occurrence. In: *Statistica* [online]. Johannes-Brahms-Platz 1, 20355 Hamburg, Germany: Ipsos Media, 2016 [cit. 2017-02-05]. Dostupné z: https://www.statista.com/statistics/291018/us-users-who-use-youtube-to-watch-or-listen-to-music/

[19] SMITH, Kit. 37 Instagram Statistics for 2016. In: *Brandwatch* [online]. 1st Floor, Sovereign House, Church Street, Brighton, BN1 1UJ: Smith, 2016 [cit. 2017-02-05]. Dostupné z: https://www.brandwatch.com/blog/37-instagram-stats-2016/

[20] SMITH, Kit. 44 Twitter Statistics for 2016. In: *Brandwatch* [online]. 1st Floor, Sovereign House, Church Street, Brighton, BN1 1UJ: Smith, 2016 [cit. 2017-02-05]. Dostupné z: https://www.brandwatch.com/blog/44-twitter-stats-2016/

[21] EDITED BY MARVIN V. ZELKOWITZ. *Advances in Computers: New Programming Paradigms (Volume 64, Advances In Computers)* [online]. 01. Amsterdam: Elsevier Science, 2005 [cit. 2017-01-08]. ISBN 00-804-5958-7.

[22] PARSON, June Jamrich. *New Perspectives on Computer Concepts 2016: Comprehensive* [online]. 18th Edition. Boston, MA: Cengage Learning, 2015 [cit. 2017-01-08]. ISBN 9781305271616.

[23] BASQUES, Kayce. Inspect and Manage Storage, Caches, and Resources: Inspect and Delete Cookies. In: *Google Developers* [online]. Mountain View, Kalifornie, USA,2017 [cit. 2017-03-22]. Dostupné z: https://developers.google.com/web/tools/chrome-devtools/manage-data/cookies

[24] KOCH, Peter-Paul. Cookies. In: *Cookies* [online]. 2017 [cit. 2017-03-18]. Dostupné z: http://www.quirksmode.org/js/cookies.html

[25] ANDREWS, Lori. *I know who you are and I saw what you did: social networks and the death of privacy* [online]. New York: Free Press, 2012 [cit. 2017-01-15]. ISBN 14-516-5051-5. Dostupné z: https://books.google.cz/books?id=XCtKe6Mjx-0C&dq=flash+cookie&hl=cs&source=gbs_navlinks_s

[26] LEVENE, Mark. *An introduction to search engines and web navigation* [online]. Hoboken, N.J: Wiley, 2013 [cit. 2017-01-15]. ISBN 11-180-6034-2. Dostupné z: https://books.google.cz/books?id=mDI72_9-bw0C&dq=flash+cookie&hl=cs&source=gbs_navlinks_s

[27] Super Cookie. In: *Techopedia Inc.* [online]. ©2017 [cit. 2017-03-18]. Dostupné z: https://www.techopedia.com/definition/27310/super-cookie

[28] PARSONS, June Jamrich. a Dan. OJA. *New perspectives [on] computer concepts 2013: social networks and the death of privacy* [online]. Second edition. Boston, MA: Course Technology, c2013 [cit. 2017-01-15]. ISBN 978-113-3190-561. Dostupné z: https://books.google.cz/books?id=19YpB6El3yAC&dq=web+bug&hl=cs&source=gbs_navlinks_s

[29] DAVIDSON, Alan. *The law of electronic commerce: social networks and the death of privacy* [online]. Second edition. New York: Free Press, 2012 [cit. 2017-01-15]. ISBN 11-075-0053-2. Dostupné z: https://books.google.cz/books?id=oXLjCgAAQBAJ&dq=web+bug&hl=cs&source=gbs_navlinks_s

[30] FLANDERS, Jon. *RESTful .NET* [online]. Sebastopol: O'Reilly Media, 2008 [cit. 2017-01-15]. ISBN 978-059-6554-330. Dostupné z: https://books.google.cz/books?id=w02As8L5l7MC&dq=etag&hl=cs&source=gbs_navlinks_s

[31] JANSSEN, Dale a Cory JANSSEN. Zombie Cookie. In: *Techopedia Inc.* [online]. ©2017 [cit. 2017-03-18]. Dostupné z: https://www.techopedia.com/definition/25736/zombie-cookie

[32] SINGEL, RYAN. *Privacy Lawsuit Targets Net Giants Over 'Zombie' Cookies* [online]. [cit. 2017-01-15]. Dostupné z: https://www.wired.com/2010/07/zombie-cookies-lawsuit/

[33] KAMKAR, Samy. Evercookie. In: *Samy* [online]. 2010 [cit. 2017-03-22]. Dostupné z: http://www.samy.pl/evercookie/

[34] TED CLAYPOOLE AND THERESA PAYTON a FOREWORD BY CHRIS SWECKER. *Protecting your internet identity: are you naked online?* [online]. Lanham, Md: Rowman, 2012 [cit. 2017-01-15]. ISBN 14-422-1220-9. Dostupné z: https://books.google.cz/books?id=SAN3f596lRAC&dq=zombie+cookies&hl=cs&source=gbs_navlinks_s

[35] Informace o modulech plug-in pro sociální sítě. In: *Facebook* [online]. ©2017 [cit. 2017-03-18]. Dostupné z: https://www.facebook.com/help/443483272359009/

[36] KYRNIN, Jennifer, Chuck HUDSON a Tom LEADBETTER. *The HTML5 Developer's Collection* [online]. USA: Addison-Wesley, 2011 [cit. 2017-01-15]. ISBN 0132911183, 9780132911184. Dostupné z: https://books.google.cz/books?id=MvCqDrCq7uYC&dq=webstorage&hl=cs&source=gbs_navlinks_s

[37] Local Storage: Sbohem cookies, sbohem session? In: *ASPNET* [online]. Pobočná 9, 140 00 Praha 4: Devel.cz Lab, 2011 [cit. 2017-03-18]. Dostupné z: http://www.aspnet.cz/articles/344-local-storage-sbohem-cookies-sbohem-session

[38] MALÝ, Martin. Webdesign: Webdesignérův průvodce po HTML5: WebStorage. In: *Zdroják, o tvorbě webových stránek a aplikací* [online]. Pobočná 9, 140 00 Praha 4: Devel.cz Lab, ©2017 [cit. 2017-03-18]. Dostupné z: https://www.zdrojak.cz/clanky/webdesigneruv-pruvodce-po-html5-webstorage

[39] ANGWIN, Julia. Meet the Online Tracking Device That is Virtually Impossible to Block. In: *PROPUBLICA* [online]. 2014 [cit. 2017-03-18]. Dostupné z: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[40] ENGLEHARDT, Steven a Arvind NARAYANAN. Online Tracking: A 1-million-site Measurement and Analysis. In: *Random walker* [online]. Princeton University, 2016 [cit. 2017-03-23]. Dostupné z: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

[41] Meet the Online Tracking Device That is Virtually Impossible to Block. In: *BrowserLeaks* [online]. ©2011-2017 [cit. 2017-03-18]. Dostupné z: https://browserleaks.com/canvas

[42] SANORITA, Dey, Roy NIRUPAM, Xu WENYUAN, Choudhury ROMIT ROY a Nelakuditi SRIHARI. *AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable* [online]. San Diego, CA, USA, 2014 [cit. 2017-01-27]. Dostupné z: http://synrg.csl.illinois.edu/papers/AccelPrint_NDSS14.pdf. University of Illinois at Urbana-Champaign, University of South Carolina and Zhejiang University, University of South Carolina.

[43] Personalizace. In: *Adaptic* [online].©2017 [cit. 2017-01-30]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/personalizace/

[44] BUŠEK, Michal. *Personalizace: nová dimenze přístupu k zákazníkovi* [online]. In: . CCB, spol. s r.o., 2001 [cit. 2017-01-30]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/clanky/personalizace-nova-dimenze-pristupu-k-zakaznikovi.htm

[45] Behaviorální marketing. In: *Mediaguru.cz* [online]. Lomnického 5, 140 00 Praha 4 [cit. 2017-02-02]. Dostupné z: https://www.mediaguru.cz/medialni-slovnik/behavioralni-marketing/

[46] SAIA, Roberto, Ludovico BORATTO, Salvatore CARTA a Gianni FENU. Binary sieves: Toward a semantic approach to user segmentation for behavioral targeting: Toward a semantic approach to user segmentation for behavioral targeting. *Future Generation Computer Systems*. 2016, 64, 186-197. DOI: http://dx.doi.org/10.1016/j.future.2016.04.006. ISSN 0167739x. Dostupné také z: //www.sciencedirect.com/science/article/pii/S0167739X16300838

[47] VAN DAM, Jan-Willem a Michel VAN DE VELDEN. Online profiling and clustering of Facebook users. *Decision Support Systems*. 2015, 70, 60-72. DOI: http://dx.doi.org/10.1016/j.dss.2014.12.001. ISSN 01679236. Dostupné také z: //www.sciencedirect.com/science/article/pii/S0167923614002796

[48] YOU, Quanzeng, Sumit BHATIA a Jiebo LUO. A picture tells a thousand words—About you! User interest profiling from user generated visual content. *Signal Processing*. 2016, 124, 45-53. DOI: http://dx.doi.org/10.1016/j.sigpro.2015.10.032.

ISSN 01651684. Dostupné také z: //www.sciencedirect.com/science/article/pii/S0165168415003758

[49] About Wolfram Alpha. In: *Wolfram Alpha LLC—A Wolfram Research Company* [online]. ©2017 [cit. 2017-03-22]. Dostupné z: http://www.wolframalpha.com/about.html

[50] Základy AdSense: Rozdíl mezi programy AdWords a AdSense. *Google* [online]. Mountain View, Kalifornie, USA, ©2017 [cit. 2017-02-18]. Dostupné z: https://support.google.com/adsense/answer/76231?hl=cs

[51] Nápověda DoubleClick Ad Exchange Seller: Rozdíly mezi službami Ad Exchange a AdSense. *Google* [online]. Mountain View, Kalifornie, USA, ©2017 [cit. 2017-02-18]. Dostupné z: https://support.google.com/adxseller/answer/4599464?hl=cs

[52] DoubleClick (Google): What is it and what does it do? *Guardian News and Media Limited or its affiliated companies* [online]. Mountain View, Kalifornie, USA, ©2017 [cit. 2017-02-18]. Dostupné z: https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring

[53] KUBÍK, Milan. Jak zvýšit dosah příspěvků na sociální síti Facebook? In: *WEBNIA* [online]. Litomyšl, 2016 [cit. 2017-02-18]. Dostupné z: https://www.webnia.cz/clanky/detail/30-jak-zvysit-dosah-prispevku-na-socialni-siti-facebook

[54] Easier, More Effective Ways to Reach the Right People on Facebook. In: *Facebook* [online]. ©2017 [cit. 2017-02-18]. Dostupné z: https://www.facebook.com/business/news/Core-Audiences

[55] Zásady používání dat: Jaké druhy informací shromažďujeme?In: *Facebook* [online]. ©2017 [cit. 2017-01-27]. Dostupné z: https://www.facebook.com/about/privacy/

[56] PARISER, Eli. *The filter bubble: what the Internet is hiding from you*. London [etc.]: Viking, 2011. ISBN 978-067-0920-389.

[57] O Lightbeam. In: *Mozilla* [online]. 2017 [cit. 2017-03-18]. Dostupné z: https://www.mozilla.org/cs/lightbeam/about/

[58] BRINKMANN, Martin. EFF launches Panopticlick 2 with new tracking and fingerprinting tests. In: *GHacks Technology News* [online]. Von-Einem-Str.52 45130 Essen, 2015 [cit. 2017-03-18]. Dostupné z: http://www.ghacks.net/2015/12/17/eff-launches-panopticlick-2-0-with-new-tracking-tests/

[59] ECKERSLEY, Peter. How Unique Is Your Web Browser? In: *Panopticlick* [online]. 2014 [cit. 2017-03-25]. Dostupné z: https://panopticlick.eff.org/static/browser-uniqueness.pdf

[60] PANOPTICLICK [online]. In: *Panopticlick* [cit. 2017-01-15]. Dostupné z: https://panopticlick.eff.org/

[61] The creepy website that tracks your every move: ClickClickClick reveals how much browsers know about you. In: *Daily Mail, The Mail on Sunday & Metro Media Group* [online]. 2016 [cit. 2017-03-18]. Dostupné z: http://www.dailymail.co.uk/sciencetech/article-3957716/The-creepy-website-tracks-ClickClickClick-reveals-browsers-know-you.html

[62] Web Browser Security. In: *BrowserLeaks* [online]. ©2011-2017 [cit. 2017-03-18]. Dostupné z: https://browserleaks.com

[63] Zásady ochrany osobních údajů. *Instagram* [online]. ©2017[cit. 2017-01-28]. Dostupné z: https://help.instagram.com/155833707900388

[64] Twitter Privacy Policy. *Twitter International Company* [online]. One Cumberland Place, Fenian Street Dublin 2, D02 AX07 IRELAND, ©2017 [cit. 2017-01-28]. Dostupné z: https://twitter.com/privacy

[65] Volba nastavení ochrany soukromí. In: *Google* [online]. ©2017 [cit. 2017-02-18]. Dostupné z: https://support.google.com/chrome/answer/114836?co=GENIE.Platform%3DDesktop&hl=cs

[66] Úprava nastavení obsahu webových stránek. In: *Google* [online]. Mountain View, Kalifornie, USA, ©2017 [cit. 2017-02-18]. Dostupné z: https://support.google.com/chrome/answer/114662

[67] 10 Ad Blocking Extensions Tested for Best Performance. In: *Raymond.CC Blog* [online]. 2017 [cit. 2017-02-18]. Dostupné z: https://www.raymond.cc/blog/10-ad-blocking-extensions-tested-for-best-performance/3/

[68] AdBlock. In: *Internetový obchod Chrome* [online]. ©2017 [cit. 2017-02-18]. Dostupné z: https://chrome.google.com/webstore/detail/adblock/gighmmpiobklfepjocnamgkkbiglidom?hl=cs

[69] Ghostery. In: *Internetový obchod Chrome* [online]. ©2017 [cit. 2017-02-18]. Dostupné z: https://chrome.google.com/webstore/detail/ghostery/mlomiejdfkolichcflejclcbmpeaniij?hl=cs

[70] M. BARRETT, Collin. FilterList. In: *FilterList* [online]. ©2017 [cit. 2017-02-18]. Dostupné z: https://filterlists.com/about/

[71] HILL, Raymond. Dynamic filtering: quick guide. In: *FilterList* [online]. 2016 [cit. 2017-02-18]. Dostupné z: https://github.com/gorhill/uBlock/wiki/Dynamic-filtering:-quick-guide

[72] O'DONNELL, Andy. How to Disable Facebook Places Location Tracking. In: *Lifewire* [online]. 2017 [cit. 2017-02-18]. Dostupné z: https://www.lifewire.com/how-to-disable-facebook-places-location-tracking-2487718

[73] Zásady pro odstraňování obsahu. In: *Google* [online]. Mountain View, Kalifornie, USA, ©2017 [cit. 2017-03-12]. Dostupné z: https://support.google.com/websearch/answer/2744324

[74] Odstranění informací z Googlu. In: *Google* [online]. Mountain View, Kalifornie, USA, ©2017 [cit. 2017-03-12]. Dostupné z: https://support.google.com/webmasters/answer/6332384?hl=cs

[75] *Nový občanský zákoník č. 89/2012 Sb.* [online]. Praha: Kurzy.cz, spol. s r.o., AliaWeb, spol. s r.o., ©2000-2017 [cit. 2017-03-12]. ISSN 1801-8688. Dostupné z: http://www.kurzy.cz/kontakty/

[76] SKLENÁK, V. *Data, informace, znalosti a Internet.* V Praze: C.H. Beck, 2001. ISBN 80-7179-409-0

[77] Cross Site Request Forgery. In: *SOM.cz* [online]. 2003 [cit. 2017-03-26]. Dostupné z: https://www.soom.cz/clanky/484--Cross-Site-Request-Forgery

[78] Document Object Model (DOM). In: *Mozilla Developer Network and individual contributors* [online]. ©2005-2017 [cit. 2017-03-26]. Dostupné z: https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model

[79] WebGL. In: *Mozilla Developer Network and individual contributors* [online]. ©2005-2017 [cit. 2017-03-26]. Dostupné z: https://developer.mozilla.org/en-US/docs/Web/API/WebGL_API

[80] Klíčové pojmy. In: *Google* [online]. Mountain View, Kalifornie, USA, 2017 [cit. 2017-03-26]. Dostupné z: https://www.google.com/policies/privacy/key-terms/

[81] HARVEY, Phil. EXIF Tags. In: *ExifTool* [online]. 2017 [cit. 2017-03-26]. Dostupné z: http://www.sno.phy.queensu.ca/~phil/exiftool/TagNames/EXIF.html

[82] Hash Function. In: *Wolfram Research, Inc.* [online]. ©1999-2017 [cit. 2017-03-26]. Dostupné z: http://mathworld.wolfram.com/HashFunction.html

[83] HTML5 Local Storage. In: *W3schools* [online]. 2017 [cit. 2017-03-26]. Dostupné z: https://www.w3schools.com/html/html5_webstorage.asp

[84] JAHODA, Bohumil. Hlavička User-Agent. In: *JE ČAS* [online]. 2015 [cit. 2017-03-26]. Dostupné z: http://jecas.cz/ua

[85] Chatujte s pomocí webRTC - 1.díl. In: PC *World on-line* [online]. Seydlerova 2451, 158 00 Praha 5: IDG Czech Republic, 2015 [cit. 2017-03-26]. Dostupné z: http://pcworld.cz/internet/chatujte-s-pomoci-webrtc-1-dil-47959

[86] DOMES, M. *Tvorba internetových stránek pomocí HTML, CSS a JavaScriptu.* Kralice: Computer Media, 2005. ISBN 80-86686-39-6

[87] SUEHRING, S. *JavaScript : krok za krokem.* Brno: Computer Press, 2008. ISBN 978-80-251-2241-9

Přílohy

Příloha č. 1 – Výsledky otisků prohlížeče v projektu Panopticlick

Browser Characteristic	Bits of identifying information	One in *x* browsers have this value	Value
Limited supercookie test	0,41	1,33	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	11,97	4019,49	0549f9b908d05b8b92b66c82d54f990c
Screen Size and Color Depth	3,13	8,73	1366x768x24
Browser Plugin Details	17,33	164799,00	Plugin 0: Citrix Receiver; Citrix Receiver Plugin (Win32); npicaN.dll; (Citrix ICA; application/x-ica; ica). Plugin 1: Citrix URL-Redirection Helper Plugin ; Citrix URL-Redirection Helper Plugin ; npURLInterceptorPlugin.dll; (; application/npurlinterceptor;). Plugin 2: Google Update; Google Update; npGoogleUpdate3.dll; (; application/x-vnd.google.update3webcontrol.3;) (; application/x-vnd.google.oneclickctrl.9;). Plugin 3: Intel® Identity Protection Technology; Intel web components for Intel® Identity Protection Technology; npIntelWebAPIIPT.dll; (npIntelWebAPIipt-2-0; application/x-vnd-intel-webapi-ipt-2.1.42;). Plugin 4: Intel® Identity Protection Technology; Intel web components updater - Installs and updates the Intel web components; npIntelWebAPIUpdater.dll; (npIntelWebAPIupdater-2-0; application/x-vnd-intel-webapi-updater; intel_webapi_updater-2-0). Plugin 5: Java Deployment Toolkit 7.0.790.15; NPRuntime Script Plug-in Library for Java(TM) Deploy; npdeployJava1.dll; (; application/java-deployment-toolkit;). Plugin 6: Java(TM) Platform SE 7 U79; Next Generation Java Plug-in 10.79.2 for Mozilla browsers; npjp2.dll; (Java Applet; application/x-java-applet;) (JavaBeans; application/x-java-bean;) (; application/x-java-vm;) (; application/x-java-applet;version=1.1.1;) (; application/x-java-bean;version=1.1.1;) (; application/x-java-applet;version=1.1;) (; application/x-java-bean;version=1.1;) (; application/x-java-applet;version=1.2;) (; application/x-java-bean;version=1.2;) (; application/x-java-applet;version=1.1.3;) (; application/x-java-bean;version=1.1.3;) (; application/x-java-applet;version=1.1.2;) (; application/x-java-bean;version=1.1.2;) (; application/x-java-applet;version=1.3;) (; application/x-java-bean;version=1.3;) (; application/x-java-applet;version=1.2.2;) (; application/x-java-bean;version=1.2.2;) (; application/x-java-applet;version=1.2.1;) (; application/x-java-bean;version=1.2.1;) (; application/x-java-applet;version=1.3.1;) (; application/x-java-bean;version=1.3.1;) (; application/x-java-applet;version=1.4;) (; application/x-java-bean;version=1.4;) (; application/x-java-applet;version=1.4.1;) (; application/x-java-bean;version=1.4.1;) (; application/x-java-applet;version=1.4.2;) (; application/x-java-bean;version=1.4.2;) (; application/x-java-applet;version=1.5;) (; application/x-java-bean;version=1.5;) (; application/x-java-applet;version=1.6;) (; application/x-java-bean;version=1.6;) (; application/x-java-applet;version=1.7;) (; application/x-java-bean;version=1.7;) (; application/x-java-applet;jpi-version=1.7.0_79;) (; application/x-java-bean;jpi-version=1.7.0_79;) (; application/x-java-vm-npruntime;) (; application/x-java-applet;deploy=10.79.2;) (; application/x-java-applet;javafx=2.2.79;). Plugin 7: Silverlight Plug-In; 5.1.20513.0; npctrl.dll; (npctrl; application/x-silverlight; scr) (; application/x-silverlight-2;). Plugin 8: VLC Web Plugin; VLC media player Web Plugin; npvlc.dll; (MPEG audio; audio/mpeg; mp2,mp3,mpga,mpega) (MPEG audio; audio/x-mpeg; mp2,mp3,mpga,mpega) (MPEG video; video/mpeg; mpg,mpeg,mpe) (MPEG video; video/x-mpeg; mpg,mpeg,mpe) (MPEG video; video/mpeg-system; mpg,mpeg,mpe,vob) (MPEG video; video/x-mpeg-system; mpg,mpeg,mpe,vob) (MPEG-4 audio; audio/mp4; aac,mp4,mpg4) (MPEG-4 audio; audio/x-m4a; m4a) (MPEG-4 video; video/mp4; mp4,mpg4) (MPEG-4 video; application/mpeg4-iod; mp4,mpg4) (MPEG-4 video; application/mpeg4-muxcodetable; mp4,mpg4) (MPEG-4 video; video/x-m4v; m4v) (AVI video; video/x-msvideo; avi) (Ogg stream;

Browser Characteristic	Bits of identifying information	One in x browsers have this value	Value
			application/ogg; ogg) (Ogg video; video/ogg; ogv) (Ogg stream; application/x-ogg; ogg) (VLC plug-in; application/x-vlc-plugin;) (Windows Media Video; video/x-ms-asf-plugin; asf,asx) (Windows Media Video; video/x-ms-asf; asf,asx) (Windows Media; application/x-mplayer2;) (Windows Media; video/x-ms-wmv; wmv) (Windows Media Video; video/x-ms-wvx; wvx) (Windows Media Audio; audio/x-ms-wma; wma) (Google VLC plug-in; application/x-google-vlc-plugin;) (WAV audio; audio/wav; wav) (WAV audio; audio/x-wav; wav) (3GPP audio; audio/3gpp; 3gp,3gpp) (3GPP video; video/3gpp; 3gp,3gpp) (3GPP2 audio; audio/3gpp2; 3g2,3gpp2) (3GPP2 video; video/3gpp2; 3g2,3gpp2) (DivX video; video/divx; divx) (FLV video; video/flv; flv) (FLV video; video/x-flv; flv) (Matroska video; application/x-matroska; mkv) (Matroska video; video/x-matroska; mkv) (Matroska audio; audio/x-matroska; mka) (Playlist xspf; application/xspf+xml; xspf) (MPEG audio; audio/x-mpegurl; m3u) (WebM video; video/webm; webm) (WebM audio; audio/webm; webm) (Real Media File; application/vnd.rn-realmedia; rm) (Real Media Audio; audio/x-realaudio; ra) (AMR audio; audio/amr; amr) (FLAC audio; audio/x-flac; flac).
Time Zone	1,85	3,61	-120
DNT Header Enabled?	1,18	2,27	False
HTTP_ACCEPT Headers	10,75	1716,66	text/html, */*; q=0.01 gzip, deflate, br cs,en-US;q=0.7,en;q=0.3
Hash of WebGL fingerprint	7,02	130,17	a4e41fd53affb34ce0b5e8dedf3399f4
Language	8,90	477,68	cs
System Fonts	5,63	49,59	Arial, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Platform	1,24	2,36	Win32
User Agent	9,99	1017,28	Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Touch Support	0,50	1,42	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0,21	1,15	Yes

Příloha č. 2 – Souhrn celkového množství nalezených signálů

Obecné rozdělení údajů		Konkrétní údaje
Údaje o uživateli	Osobní údaje	jméno, příjmení, e-mailová adresa, fotografie, telefonní číslo, číslo kreditní nebo debetní karty, datum vypršení platnosti karty, CVV kód, fakturační adresa a jiné informace o platbě

Obecné rozdělení údajů		Konkrétní údaje
	Interakce s webovou stránkou	hashtag, geotag a komentáře, čas navštívení webové stránky, maximalizace aktuálního okna, akceptace cookies, pohyby kurzoru na aktuální stránce, kde se kurzor zdržuje, na jaké tlačítko a plugin je kliknuto, čas strávený na webové stránce
	Informace o poloze	adresa, stát/region, země, zeměpisná šířka a délka, přesnost, čas pořízení, informace o lokaci
Údaje o zařízení	Informace z protokolu (mobilního telefonu)	vyhledávací dotazy, informace z protokolu telefonování jako uživatelské telefonní číslo, číslo volajícího, číslo přesměrování, čas a datum hovorů, trvání hovorů, údaje o směrování zpráv SMS a typy hovorů, adresa internetového protokolu, informace o událostech zařízení jako selhání, činnost systému, nastavení hardwaru, typ prohlížeče, jazyk prohlížeče, datum a čas uživatelského požadavku nebo odkazující adresa URL
	Technické údaje/data	IP adresa, hostname, lokace IP adresy, poskytovatel internetových služeb, organizace, ASN, časové pásmo, místní čas, informace o WebRTC, Flash přehrávači, TCP/IP otisku, DNS serveru, hlavičce HTTP, detekce JavaScriptu/zda je používán, dokument odkazujícího serveru, User-Agent, užívaný webový prohlížeč, rozhraní stavu baterie a Web Audia, přístupové rozhraní, rozhraní o sítových informacích, informace o supercookies, instalované pluginy, navigační načasování rozhraní, podpora WebGL, Flash přehrávače, povolení cookies, Touch Support, systémové fonty, nastavení Do Not Track,Canvas fingerprint - jedinečnost User-Agenta a jeho otisku, podpis autorova jedinečného otisku prohlížeče, zda byl otisk nalezen v databázi, zobrazení, jedinečnost a velikost otisku, otisk SHA256, hlavičku PNG souboru, model hardwaru, verze operačního systému, jedinečný identifikátor zařízení, údaje o mobilní síti, ebové úložiště prohlížeče, mezipaměť aplikací, rozlišení obrazovky, datum, čas zařízení