

Tony Fish

DIGITAL FOOTPRINTS

Digital Footprints

Překlad:

Jaroslava Žgáničová

Abstrakt:

Překlad prezentuje kapitolu z e-knihy *My Digital Footprint* od Tonyho Fische, která je volně k přečtení v angličtině na internetu. Kniha představuje definici digitálních stop, která pokrývá zachycení, uchování, analýzu a hodnotu, bere v úvahu také sociální vliv a vliv třetí strany na naši digitální stopu. Vybraná kapitola vysvětluje myšlenku *Mé digitální stopy*, proces jejího budování, vstupy a výstupy a smyčku zpětné vazby, kterou se celý proces řídí. Zmínka je také o paradoxu soukromí a konceptu využívání kolektivní inteligence.

Klíčová slova: soukromí na internetu, kyberprostor, kolektivní inteligence, Internet, Digitální stopy, definice

Kapitola *Digitální stopy* je převzata z knihy *My Digital Footprint*, která je volně dostupná na internetu na adrese: <http://31.222.183.71/footprint-ugc/>. Tento překlad podléhá **Creative Commons "Uveďte autora, neužívejte komerčně"**.

Digitální stopy

Stejně jako Neil Armstrong kráčející po Měsíci nebo Nelson Mandela, když opouštěl po svém propuštění na svobodu Robben Island, my všichni po sobě zanecháváme stopy. Stopy jsou víc než identita. Stopy vypovídají o tom, kde jsme byli, po jakou dobu, jak často a také o vzájemných vztazích. Jsou to vzpomínky a okamžiky. Digitální stopy proto nelze ztotožnit s naší identitou, cestovním pasem, bankovním účtem nebo číslem sociálního pojištění. Digitální stopy vznikají na základě našich interakcí s mobilem, webem a televizí a jsou tvořeny digitálními daty a metadaty¹ (daty o datech) vypovídajícími o tom, kdo jsme. Lze za nimi vidět skutečnou hodnotu a vlastnictví tohoto druhu dat je bitevním polem, na němž můžeme zvítězit i prohrát.

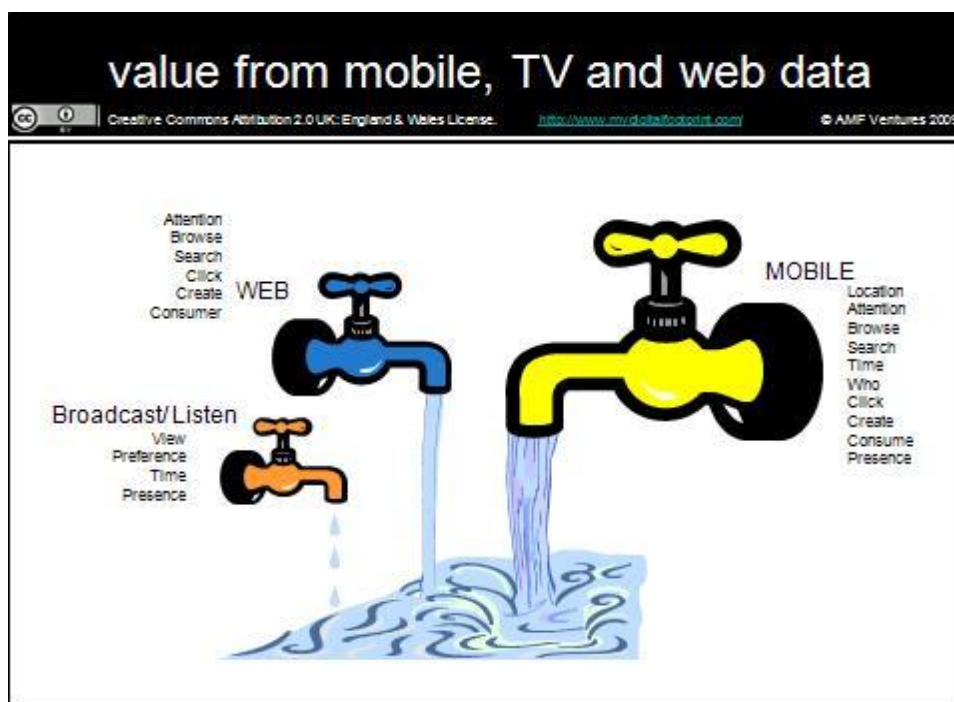
Původní digitální stopa, jejímž východiskem byl web a digitální data s ní spojená, patřila v určité fázi jednotlivci. V současnosti ale není v moci jednotlivce tuto digitální stopu vlastnit nebo řídit. Mobilní technologie rozšiřují digitální stopu o jedinečnou dimenzi, neboť s nimi přichází nový obsah, metadata a zasazení digitální stopy do sociálního kontextu. Zatímco televize a web mohou poskytnout určitá data, mobilní zařízení jsou oproti nim ve způsobu, jakým přispívají k naší digitální stopě, naprosto unikátní. Tuto myšlenku ilustruje obrázek 6. Kohoutky a objem vytékající vody představují vizualizaci velikosti hodnoty, která může být vytvořena na základě uživatelských

¹ <http://en.wikipedia.org/wiki/Metadata> July 2009

dat. Voda plní nádrž znázorňující digitální data, která jsou o vás ukládána na základě vašich interakcí.

Data získaná ze zdroje, který můžeme označit jako „Vysílání/Poslech“, zahrnují následující informace: časy sledování a harmonogramy, preferované kanály a obsah, načasování programů a přítomnost (zda jste skutečně u přijímače, což se dá určit na základě pohybu, přepínání mezi kanály, rychlého přetáčení dopředu nebo druhotného zařízení, osobního počítače nebo mobilu, který bude sledovat vaše televizní preference).

Data získaná z webu zahrnují: pozornost, informaci o tom, jak dlouho jste si četli konkrétní stránku, historii prohlížení, vyhledávaná slova a pravopis, vzorce a kliknutí, vytvořený nebo zhlédnutý obsah a nákupy (konzumování). Data z mobilního zařízení by pak zahrnovala: polohu, pozornost, prohlížení, vyhledávání, čas, informaci o tom, s kým jste (Bluetooth), blízkost, kliknutí, vytváření dat a média, spotřebitele, playlisty a přítomnost. Vlastními surovými daty by mohly být souřadnice místa, na kterém se nacházíte, kliknutí, obousměrné interakce nebo fotografie. Velikost kohoutku a proudu znázorňuje objem dat, který může přitéct do zásobníku digitálních stop.



Obrázek 6 Hodnota vytvářená na základě mobilního zařízení, televize a webu

Od digitálních stop k MOJÍ DIGITÁLNÍ STOPĚ

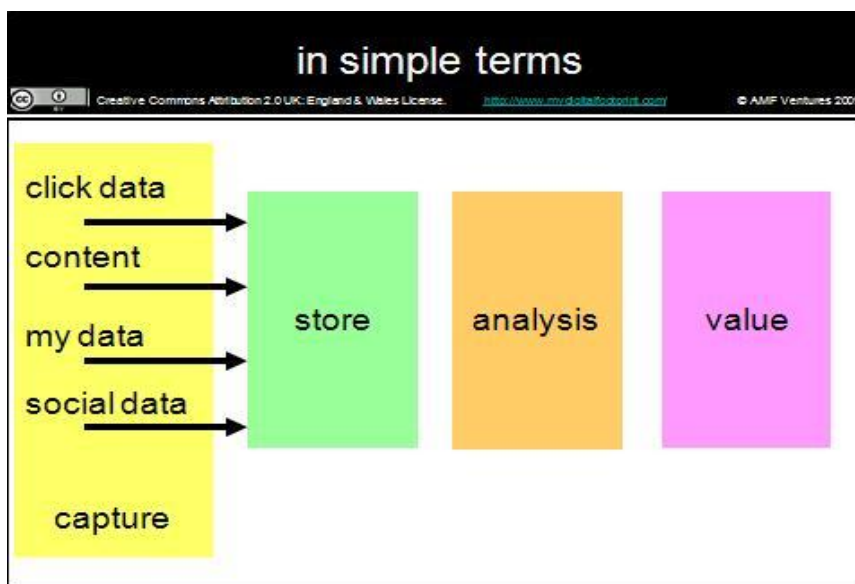
Myšlenka digitálních stop byla věnována pozornost z pohledu ochrany soukromí nebo dat. Klíčoví komentátoři se však shodují, že digitální stopy, které po sobě zanecháváme, se neustále zvětšují, zvláště vezmeme-li v úvahu, jakým způsobem roste obliba sociálních sítí a mobilních zařízení.

Digitální stopa je přetrvávání datových stop on-line v důsledku aktivity uživatele v digitálním prostředí – což je jev, který Nicholas Negroponte ve své knize *Being Digital*² označil jako „slug trail“³ a který John Battelle⁴ nazývá „clickstream exhaust“⁵.

Podle zprávy Pew Internet⁶ lze digitální stopy rozdělit do dvou hlavních kategorií: pasivní digitální stopy a aktivní digitální stopy. Pasivní digitální stopa vzniká v situaci, kdy dojde ke sběru dat ohledně konkrétního úkonu bez jakékoli aktivace ze strany zákazníka (implicitní), a zahrnuje data získaná prostřednictvím senzorů. Naproti tomu aktivní digitální stopy vznikají, pokud uživatel záměrně zveřejní osobní údaje za účelem sdílení informací o sobě (explicitní).

Na webu tak mnohé interakce, jako například vytvoření profilu na sociální síti nebo vložení komentáře k fotografii na Flickru, zanechávají digitální stopu. V mobilním kontextu je digitální stopa uživatele tvořena transakčními daty v podobě záznamů o hovoru, tzv. CDRs (Call Data Records). Avšak pouhá dostupnost transakčních dat jako taková nestačí, protože se na užití těchto dat vztahují pravidla na ochranu soukromí a dat, což je také správné. To, čím se zkoumání digitálních stop liší, je schopnost uchovat, analyzovat a vytvářet hodnotu na základě digitální stopy. Jinými slovy, pokud bychom všichni zanechávali po sobě digitální stopy, aniž by se s nimi cokoli dělo, pak by nebyl důvod k jakýmkoli obavám, ani k očekávání jakéhokoli přínosu.

V této knize proto představujeme definici digitálních stop, která pokrývá zachycení, uchování, analýzu a hodnotu. Fázi „zachytávání“ netvoří pouze vaše vlastní aktivita, ale také aktivita dalších lidí spojených s příslušným informačním prvkem – např. vliv vašeho sociálního grafu a třetích stran na vaši digitální stopu. Tuto myšlenku ilustruje obrázek 7.



Obrázek 7 Definování složek vytvářejících digitální stopu prostřednictvím jednoduchého schématu.

² česky vyšlo pod názvem „Digitální svět“ – pozn. překl.

³ „slug“ je zde použito ve významu technických poznámek používaných v průběhu zpracovávání dokumentu, zároveň spojení „slug trail“ má v angličtině význam „slimáčí stopa“ – pozn. překl.

⁴ <http://battellemedia.com/archives/000647.php>

⁵ volně přeloženo: to, co do digitálního prostředí „vypouštíme“ clickstreamem (tj. spojitým tokem kliknutí) – pozn. překl.

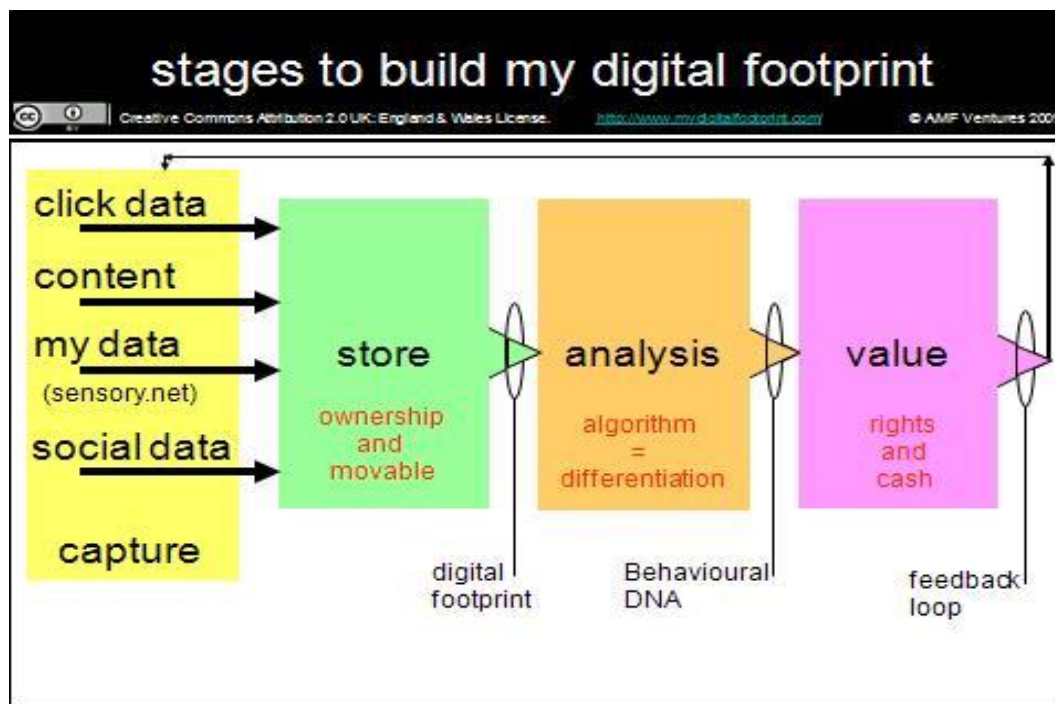
⁶ <http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx>

Data jsou zachycována z různých zdrojů, a tedy, což je dobré zdůraznit, nikoli pouze z dat vytvořených daným člověkem, ale i prostřednictvím senzorů zabudovaných v zařízeních nebo k nim připojených. Uchování digitální stopy je spojeno s tím, kde jsou fyzicky uložena surová data. Jde tu o vlastnictví a přenositelnost [analýza je také uchována, ale nelze z ní zpětně získat surová data a identifikovat uživatele, polohu, službu, nákup nebo jakýkoli jiný jedinečný prvek]. Analýza je rozhodujícím faktorem, pokud jde o to, kde by mohlo vzniknout bohatství, a je také spojena s potenciální hodnotou, jíž může využít uživatel i poskytovatelé služeb.

Zachycená data jsou tak tvořena daty odvozenými na základě kliknutí (digitální stopa) a obsahu (vlastní vytvořená data – např. fotografie nahrané z mobilního zařízení). Moje data, jak je znázorněno na obr. 8, představují automatizovaný sběr dat, který může mít podobu vložené pozice ve fotografii nebo může být v některých aplikacích povolen uživatelem. Součástí mých dat je sensory.net, kdy zařízení funguje jako senzor a shromažďuje informace. Posledním vstupem je pak sociální složka. Sociální složku nepředstavují vaše data o vás po vzoru ostatních vstupů. Sociální data jsou to, co o vás jako o jednotlivci poskytne vaše sociální skupina; vaše reference na LinkedIn, vaše hodnocení na eBay, označení vašich fotografií na Flickru a na Facebooku.

Mezi „digitálními stopami“ – tj. mezi surovými daty, která jsou zachycena a uchována pro analýzu – a mojí digitální stopou, existuje jemný, ale významný rozdíl. Myšlenka mojí digitální stopy je rozšířením myšlenky surových dat na širší koncept zachycení, uchování, analýzy a hodnoty vytvořené z dat generovaných prostřednictvím zapojení se do digitálního světa. Koncept mojí digitální stopy nám umožňuje zaměřit se na systém a hodnotu, která je vytvářena.

Tento proces budování **MÉ DIGITÁLNÍ STOPY** je založen na strukturovaném přístupu, který v sobě zahrnuje vstupy (shromažďování) a výstupy (hodnota) a smyčku zpětné vazby, kterou se celý proces řídí. Kdo stojí za tímto budováním, je důležitá otázka, které se budeme věnovat v této knize v kapitole o byznys modelech. Zmíněná smyčka zpětné vazby postupně obohacuje a třídí výstupy (hodnotu). Fáze analýzy umožňuje vzít surová data z různých uložených zdrojů (které označujeme jako digitální stopu) a na základě analýzy těchto surových vstupů vytvořit hodnotu (statky a služby), jež má podobu takových složek jako personalizace, reputace nebo objevování. Výstup této analytické fáze nazýváme „behaviorální DNA“, a to proto, že poskytuje váš podrobný popis, ale neplyne vám z ní žádná hodnota.



Obrázek 8 Definování jednotlivých stádií vytváření MÉ DIGITÁLNÍ STOPY

Podrobný popis vstupů a výstupů a také toho, jakým způsobem funguje smyčka zpětné vazby, je uveden v kapitole věnované dvoustrannému byznys modelu. Zde uvedeme alespoň stručný popis vstupů a výstupů. Vstupy **MÉ DIGITÁLNÍ STOPY** jsou datové prvky a výstupy tvoří hodnota odvozená z procesu, který je zase obohacen prostřednictvím smyčky zpětné vazby.

Vstupy MÉ DIGITÁLNÍ STOPY

Pozornost

Data, z nichž vyplývá, co děláte. Jde o poskytování dat obsahujících informace o tom, jaké aplikace a služby využíváte. Tuto roli může plnit nějaké příslušenství na vašem stolním počítači, mobilu nebo set-top boxu, které poskytuje přehled o tom, jaké aplikace jsou otevřené, jak dlouho jste upravovali konkrétní dokument, na které fotografie jste se dívali, jakou hudbu jste poslouchali a jak často. Datový tok týkající se pozornosti je záznamem o způsobech, jakým trávíte svůj čas v digitálním světě, ať už se jedná o televizi, web nebo mobilní zařízení.

Poloha

Datový záznam o tom, kde se nacházíte. Vstupy získávané v reálném čase představují sběr. Pokud jsou data uložena, poskytují informace o tom, kde jste se nacházeli (zvolenou trasu).

Čas

Záznam časových dat obsahuje jednak informaci o čase v rámci dne, jednak o příslušném období.

Vyhledávání

Datový řetězec požadavků na vyhledání, v současné době slova textu (a hlasové vyhledávání na Google Mobil) zadaná do vyhledávače, postupně však stále více nabývá podob automatizovaného vyhledávání na základě požadavků z 3D čárových kódů a informací dostupných v místě.

Obsah (vytváření)

Datový záznam typu, kontextu a informací o obsahu, který jste vytvořili, a to pro text, hlasový materiál, prezentaci, hudbu, zvukový materiál, obrazový materiál, video, blogy, tagy a doporučení.

Aktivita

Tento soubor dat definuje, co děláte. Zatímco pozornost říká, že se díváte na konkrétní webovou stránku, aktivita určí, že jste na fotbalovém hřišti. Poloha pak vypovídá o vašich souřadnicích.

Výstupy – hodnota vytvořená z digitálních stop

Záměr

Záměr je výstup, který poskytuje výpověď o tom, co se chystáte dělat na základě toho, co jste dělali, co dělá váš sociální graf, ale také na základě toho, co jste řekli/vyvodili/naznačili, že se chystáte dělat. To může vyplývat např. z vašeho kalendáře, e-mailu nebo stopy zanechané prostřednictvím instant messaging. Zatímco kontext se vztahuje k aktuálnímu okamžiku, záměr se dívá do budoucnosti.

Reputace

Reputace (digitální) má mnoho složek. Reputace je dána jednak hodnocením (dobré nebo špatné) a jednak vaší vlastní tendencí jednat určitým způsobem, například přidávat komentáře. Reputace (digitální) proto zčásti vypovídá o hodnotě, jakou máte pro vaši komunitu jako účastník.

Výsledkem těchto výstupních dat je záznam, který představuje vaši digitální reputaci.

Objevování

Tento výstup zahrnuje koncepty, myšlenky a vhled, které umožňují uživateli objevovat. Objevování je úzce spojeno s rizikem a má podobu vylepšování stávající služby nebo objevení nové služby/aplikace.

Doporučení

Toto je možnost, je kdy služba/aplikace na základě vaší digitální stopy (vy a váš sociální graf) schopná provést doporučení o stávajícím nebo novém produktu či službě s mírou jistoty, díky níž bude takové doporučení relevantní. Jestliže při objevování jde o riziko, základem doporučení je důvěra.

Ochrana

V tomto případě jde o to, že vaše data mohou sloužit k ochraně vás a vašich dat stejným způsobem, jako je tomu v případě podvodů s kreditními kartami. Vaše data jsou dobrým vodítkem, pokud jde o určení, zda osoba, která data poskytuje, jste opravdu vy. Možnost využít data tímto způsobem je dána tím, že lidé a určité sociální skupiny jsou otroky zvyku.

Personalizace

Jde o případy, kdy je aplikace nebo služba personalizována pro konkrétního uživatele pro určitý případ nebo čas. Jedná se o automatickou úpravu generické služby, ovšem na základě toho, co je o vás známo.

Obchod nebo barter

Tato funkce výstupu druhého řádu umožňuje uživateli obchodování se zbožím nebo službami nebo jejich směnu. Obchod nebo barter nebude probíhat za peníze (platbu), ale za data nebo určité vhledy, výzkum atd. Tento typ obchodu nebo barteru je založen na vstupních datech, analýze, záměru a reputaci.

Kontextuální adaptace

Zde jde o přizpůsobení služby nebo aplikace tak, aby byla poskytnuta služba, která je jedinečná s ohledem na požadavky jednotlivce vycházející z existujícího prostředí.

Paradox soukromí

Soukromí je spojeno s jistým paradoxem. Na jedné straně mají všichni strach z jeho ztráty. Scott McNealy ze Sun Microsystems se zapsal do povědomí svým výrokem na toto téma: „Soukromí spotřebitelů je falešná stopa: žádné soukromí nemáme – a měli bychom se s tím vyrovnat”⁷. To je pohled, který získal na věrohodnosti po 11. září 2001. Esther Dyson zdůrazňuje, že potřebujeme mít detailnější kontrolu nad svými daty. Je přesvědčená, že pojem soukromí nepostihuje plně výzvy současného on-line prostředí. „Potřebujeme přestat mluvit o soukromí a začít mluvit o kontrole nad našimi daty,“ říká. A dodává, že „v budoucnu budou uživatelé chtít mít mnohem hlubší

⁷ <http://www.wired.com/politics/law/news/1999/01/17538>

kontrolu nad svými daty a budou do větších detailů rozhodovat o tom, co budou s kým sdílet. Uživatelé mohou být ve chvíli, kdy si zřizují svůj účet, ohromeni, ale jakmile si na aplikaci více zvyknou, začnou uplatňovat ve větší míře kontrolu.“

Pokud se zvláště zajímáte o otázky soukromí, pak stojí za to přečíst si o myšlence detailní kontroly nad našimi osobními údaji více, zejména práce Kima Camerona⁸ a Stefana Brands⁹. Typ revidovaného technického modelu, jaký je zakotven v pravidlech identity, v kombinaci s chytrou kryptografií tokenů zpřístupňujících minimum identifikačních údajů („minimal disclosure tokens“) znamená (alespoň na technické úrovni) významný průlom ve způsobu, jakým uvažujeme o inženýringu designu digitálních produktů a služeb a o tom, jak umožnit uživateli, aby měl nad svými daty díky své silné pozici velmi detailní kontrolu.

Na druhou stranu jsme k poskytování údajů o sobě všichni motivováni představou větší viditelnosti v digitálním kontextu, přičemž máme možnost uvažovat o tom, jakým způsobem chceme být vnímáni. Například, i když nechceme zanechat žádnou digitální stopu, chceme být přesto na webu vyhledatelní a dáváme přednost tomu, aby nás výsledky ukazovaly v dobrém světle.

A tak buď pasivně vytváříme digitální stopy, nebo aktivně přispíváme informacemi o sobě. V obou případech přispíváme k tomu, jaký si o nás někdo vytvoří názor, ale zároveň se tím vzdáváme dat a naší digitální stopy, která by mohla být využita.

Kdo využívá vaši kolektivní inteligenci?

Web 2.0 nás naučil používat koncept „využívání kolektivní inteligence“, kterému se budeme podrobněji věnovat v této části. Využívání kolektivní inteligence nepředstavuje problém samo o sobě. Temná stránka se však začne projevovat, pokud se nějaký subjekt snaží přimět svoje publikum (zákazníky, klienty, delegáty, pacienty, přátele), aby se vzdali svých digitálních dat, shromažďuje jejich digitální stopu bez jejich souhlasu, účtuje uživatelům poplatky za prohlížení jejich vlastních dat nebo prodává NAŠE data čistě proto, aby vydělal na jednostranném využívání. Moje mobilní číslo [tj. Tonyho Fishe] je volně dostupné na webu a nikdy na něm nemám žádné nežádoucí hovory; číslo mého telefonu domů není v seznamu, je uvedeno pouze v soukromých aplikacích a jednou týdně mi někdo volá s obtěžující obchodní nabídkou, tak se ptám, kdo prodal moje data?

1. května 2009 skončila služba Spock¹⁰ v rukou společnosti Intelius (společnost specializující se na prověřování osob). Spock je založen na robotovi, který automaticky vytváří tagy pro jakoukoli nalezenou osobu. Pátrá v takových vodách webu, jako jsou stránky Wikipedie, LinkedIn a další. Také umožňuje uživatelům doplnit svá data přidáním vlastních tagů a dalších dat, jako například vztahů mezi lidmi. A tak se stránka postupně zlepšuje, v duchu myšlenky Webu 2.0, s tím, jak ji využívá více lidí. Nicméně z pohledu uživatele je to trochu ošemetné, protože:

- Spock prohledává web, aby našel naše data;

⁸ <http://www.identityblog.com/>

⁹ <http://www.idcorner.org/>

¹⁰ www.spock.com

- vytváří o nás profil na jejich stránce bez našeho výslovného souhlasu;
- vyzývá nás k tomu, abychom tyto informace doplnili;
- účtuje nám poplatek za přístup k našim vlastním informacím; a
- nakonec prodá ty samé informace společnosti zabývající se prověřováním osob.

Otevřená zůstává otázka, zda mohu své vlastní informace na Spocku smazat. A tady to v mnoha ohledech začíná být zajímavé. Ohledně smazání informací uvádí Spock toto¹¹:

„Pokud si přejete odstranit informace o vás ze služby Spock, prosím přečtěte si následující informace a klikněte na níže uvedený odkaz. Před tím, než požádáte o odstranění, je potřeba zajistit, aby původní zdroj informací, který o vás Spock našel, byl odstraněn nebo přestal být veřejný (MySpace, blog, Friendster atd.). Tím zamezíte, abyste byl/a opětovně zahrnut/a do indexace na těchto stránkách. Upozorňujeme, že lze požádat pouze o odstranění vašeho výsledku vyhledávání na Spocku. Při vyplňování vašich údajů prosím zkontrolujte, že jste uvedl/a svoje jméno, e-mail a odkaz na váš výsledek vyhledávání na Spocku (<http://www.spock.com/Tiger-Woods>) a také důvod, proč nechcete již být do služby zahrnut/a. Tým podpory služby Spock posoudí vaši žádost a zkontaktuje vás do 24-48 hodin.“

Co z toho vyplývá, je, že já jako uživatel musím zajistit, aby původní zdroje informací, které oni (Spock) využili jako zdroj (přes robota) pro vytvoření profilů, přestaly být veřejné (můj blog, můj profil na Facebooku atd.), jinak mě opět „využijí“. Toto je v rámci Webu 2.0 ekvivalent získávání e-mailových adres a jejich další prodej.

Je možné, že v budoucnu bude legislativa doplněna způsobem, který pokryje i tyto praktiky, a myšlenka silnějšího postavení zákazníka se dostane širšího přijetí. Vzhledem ke stále větší dostupnosti mobilních zařízení nabývají tyto otázky spolu s Mobilním Webem 2.0. na významu. (Mobilním Webem 2.0 mám na mysli koncept rozšíření myšlenky využívání kolektivní inteligence na mobilní zařízení, která jsou lépe uzpůsobená zachycovat data společně s doprovodnými metadaty.) Z trochu optimističtějšího pohledu se ale dá říci, že užívání dat vytvořených uživatelem za účelem vytvoření lepší služby je dobrá věc, za předpokladu, že jde o transparentní proces, nad kterým má uživatel kontrolu.

A tak i když byly principy Webu 2.0 správné, některé realizace tohoto byznys modelu nutně být nemusí, zvlášť pokud jsou BEZPLATNÉ. Zodpovědné společnosti budou tyto principy využívat k vytváření lepších služeb (a budou web a mobilní zařízení využívat holisticky). Tyto služby možná nebudou bezplatné, a tudíž ani odpovídat označení „Web 2.0“ v tradičním významu. Budou ale poctivější ve vztahu ke svým zákazníkům a s daty svých zákazníků budou nakládat transparentněji. Také uživatelé mohou být časem moudřejší a získat silnější pozici. Poučíme se z chyb Webu 2.0 a dosáhneme vyšší úrovně zapojení uživatelů a důvěry, která bude založena na konvergováných/mobilními technologiemi inspirovaných službách.

¹¹ <http://www.spock.com/do/pages/help#claim-search-result>

Soukromí – je vaše soukromí věcí někoho jiného?

Debata, kterou jsme nastínili výše, nás přivádí k otázce: „Stává se naše soukromí věcí někoho jiného?“ Mám na mysli asi toto: využívají společnosti moje soukromá data pro vlastní prospěch a znamená to, že soukromí, které jsem si myslel, že mám, buď nikdy neexistovalo, nebo bylo oslabeno?

Tyto praktiky (využívání dat) přitáhly pozornost regulačních orgánů, mimo jiné například Federální obchodní komise (Federal Trade Commission) v USA¹². Obecně se má za to, že obyvatelstvo bere roli médií a značek jako samozřejmou. Marketéři vám řeknou, že „značky nás potřebují stejně jako my je“.

Značky stojí v současnosti za velkým množstvím technologií a inovací (stačí připomenout iPod), přičemž zájmy značek nejsou vždy sladěny se zájmy zákazníků. Proto je nutné pojetí, v němž „my potřebujeme značky a značky potřebují nás“ korigovat základní realitou, která spočívá v tom, že primárním účelem značek je prodávat. A na to bychom neměli zapomínat. S tím, jak narůstá bohatství a složitost médií, usilují značky o to, nás nějak zapojit a míru tohoto zapojení změřit, aby mohli maximalizovat svoje tržby. A proto také mají zájem na „využívání digitální stopy“ a z něho vyplývajícím vlivu na soukromí. Digitální stopy a soukromí, důvěra a riziko jsou dvě strany téže mince. Existují mezi nimi vazby a přemostění, jak bylo zmíněno dříve. Rozsáhlejší kapitola o těchto vztazích je uvedena ke konci knihy v návaznosti na to, jak se pozornost přesouvá na konkrétní byznys model. K tomu, aby mohly reklamní společnosti svoji reklamu více personalizovat (a potažmo žádat více peněz od společností, které jejich reklamu využívají), potřebují spoustu dat. Získávání dat ale vyžaduje, aby se zákazníci vzdali některých svých práv na soukromí, důvěřovali někomu a podstupovali určité uvážené riziko, to vše v zájmu reklamního byznysu.

Zamyslete se nad důrazem, jaký toto odvětví klade na „konvergenci“. Konvergence by mohla ve světle využívání digitální stopy nabýt mnohem temnější význam. Pokud by si média a reklamní subjekty měly opravdu „spojit jednotlivé body“ mezi různými informačními prvky, které po sobě zanecháváme (informace v různých typech médií v podobě drobků z cookies), pak by se reklama stala opravdu mocným a personalizovaným nástrojem. To zvýhodňuje reklamní subjekty zejména ve scénáři konvergovaných médií (kde účastníci platí za televizi, pevnou linku i mobilní služby témuž poskytovateli). Takový vývoj by ale mohl vést ke spornému jednání, jež by za současného stavu sice mohlo být legální, ale brzy by se mohlo stát předmětem regulace. A mohlo by to také vyvolat odpor spotřebitelů, jak bude vysvětleno v níže popsaném scénáři.

Předpokládejte, že jste fanoušek rockové skupiny a píšete o ní blog. Zamyslete se nad touto situací. Celá řada televizních společností hledá způsoby, jak „personalizovat“ televizní reklamu pro domácnosti. Například usilují o to, zjistit divácké preference ze set-top boxů a dalších nástrojů a poté (v extrémním scénáři) ušít reklamu na míru každé domácnosti. Otázka zní: Které datové prvky lze využít při vytváření reklamy na míru?

Podívejme se na složku dat představovanou „rockovým koncertem“, kterou lze získat přes RSS kanál z mého blogu. Je snadné zkombinovat tři soubory dat: adresu mého bydliště a moje jméno,

¹² http://www.forbes.com/2009/01/12/mobile-marketing-privacy-tech-security-cx_ag_0113mobilemarket.html

keré má kabelová společnost k dispozici, s RSS zdrojem z mého blogu (který je spojen s mým jménem, nebo přes prohlídku paketu s mojí virtuální identitou (personou)) a telefonním seznamem/registrací voliče (jako potvrzení mé adresy). Pokud disponuje společnost poskytující službu kabelové televize těmito informacemi, může si spojit jednotlivé body (v terminologii této knihy provést analýzu) a následně „personalizovat“ reklamu přesně na míru (odvysílat mi v reklamní pauze v televizi/kabelové televizi reklamu na další rockový koncert od daného umělce). Dá se očekávat, že by z toho měla reklamní společnost „velkou radost“, protože by se jí podařilo „personalizovat“ mně určenou reklamu a já bych se do ní dokonce mohl „zapojit“ stisknutím tlačítka „Koupit“ (reklamní utopie!). Na druhou stranu by to mohlo být vnímáno jako obrovský zásah do soukromí a sporná taktika typu „Velkého bratra“, což je také důvod, proč je prvním slovem této knihy slovo „Marmite“ – zkrátka některým se tahle myšlenka líbí, jiným ne.

Personalizace a zapojování uživatelů by mohly v budoucnu nabývat ještě horších podob vzhledem k rostoucí dostupnosti různých souborů dat, s nimiž mohou reklamní subjekty pracovat a které by mohly vzájemně propojovat s cílem získat o nás nové informace a „prodávat“ nám. Tato schopnost zpětné identifikace nebo dokonce identifikace opravdu vyvolává důležité otázky ohledně soukromí. Mohli bychom to nazvat „mikropřesvědčováním“. V každém případě nás to přivádí k otázkám reklamní etiky a etiky, kterou se řídí zapojování uživatelů (přestože by žádné z popsaného jednání nebylo vnímáno jako nelegální). Také to však vede k celé škále zákaznického odporu (např. pokud bych takových reklamních spotů na rockové koncerty zhlédl celou řadu, uvědomil bych si, že mě moje televize sleduje, a zachoval bych se podle toho, například bych změnil kanál nebo poskytovatele služeb).

Obdobně se budou chovat také vlády. Je potřeba, aby se vlády angažovaly dvěma způsoby:

- vytvořením regulace, která dává jisté výhody také spotřebitelům, nejen reklamním subjektům, zejména pokud jde o nové oblasti, v nichž regulace prakticky chybí a spotřebitelům hrozí nebezpečí, že budou využíváni; a
- zajištěním ochrany práva na soukromí jednotlivců ve světle stále narůstajících zásahů do těchto práv ze strany značek a reklamních subjektů.

Je pravda, že ve Velké Británii máme například takové zákony, jako je zákon na ochranu údajů (Data Protection Act)¹³. Na druhou stranu ale může být vláda součástí problému, například když se podíváme na předkládaný zákon o „sdílení dat“ ve Velké Británii. Pod záminkou toho, že „hromadná výměna dat může přinést výhody (reklamním subjektům a vládám) předkládá britská vláda legislativu (zdroj: webové stránky deníku Telegraph¹⁴), na jejímž základě by data, která má v držení policie, národní zdravotní služba (NHS), školy, HMRC (daňové úřady), místní samospráva a úřad spravující registr vozidel a řidičů (DVLA), mohla podle organizace Privacy International skončit v soukromých rukou. Zároveň by však podle jejího tvrzení mohly být vládě předávány informace shromážděné společnostmi, mimo jiné například hotelové registrace, bankovní údaje a telekomunikační data, a to na základě ustanovení zákona o práci koronera a soudnictví (Coroner's

¹³ http://en.wikipedia.org/wiki/Data_Protection_Act_July_2009

¹⁴ <http://www.telegraph.co.uk/news/newstopics/politics/4339771/Threat-to-privacy-under-data-law-campaigners-warn.html>

and Justice Bill). Skupina, která vede kampaň, připouští, že „hromadná výměna osobních údajů má potenciál přinést jistý užitek.“

Další oblastí bez dostatečné úpravy je reklama zacílená na nezletilé a na etnické skupiny. Z právního hlediska neexistuje žádná norma zakazující zacílení reklamy na konkrétní etnickou skupinu. Takový postup může být ve skutečnosti výnosný, podle toho jak o tom referuje reklamní síť JumpTap, která zveřejnila své očekávání, že kampaň zaměřená na hispánské obyvatelstvo se v letošním roce zčtyřnásobí, přičemž tržby v tomto segmentu by měly stoupnout minimálně o 20 %¹⁵. Na prodeji hispánsky orientovaného obsahu, hudby atd., tj. prodeji zaměřeném na konkrétní demografickou skupinu, nemusí být nutně nic špatného, ale pozměňme ten model jenom trochu a už jsou na místě vážné obavy o soukromí. Faktem například je, že obyvatelé jižní Asie jsou geneticky náchylní k cukrovce¹⁶. Znamená to, že by se měla reklama na léky na cukrovku v Británii zaměřit na osoby pocházející z jižní Asie? A opět je řeč o něčem, co dnes není příliš složité zrealizovat za použití současných technologií a díky rostoucí konvergenci a dostupnosti dat. Kde tedy stanovit hranici?

Televizní reklama na léky je pro mnohé z nás, kteří cestují do Spojených států, běžnou realitou. Přitom v řadě zemí je toto nelegální – zejména v Evropě. Zdá se, že těmto reklamám je společně sdělení ve smyslu „Zavolejte svému praktickému lékaři a požádejte ho, aby vám doporučil naše léky.“ Vysílání reklam farmaceutických společností je spojeno s etickým problémem, který spočívá v tom, že společnost využívající reklamy se snaží ovlivnit úsudek lékaře z komerčních důvodů (aby prodala své produkty). V řadě zemí je toto považováno za etickou otázku, která podléhá určité formě regulačního dohledu.

Další oblastí, kterou je potřeba zmínit, je ochrana nezletilých. A zvláště v éře, jíž dominují mobilní technologie a sociální sítě. Sociální sítě, mobilní zařízení a další nová média nabízejí možnost posunout hranice reklamy zaměřené na děti. Opět platí, že tyto praktiky nejsou nelegální (zatím!), ale jsou zcela jistě sporné z morálního hlediska. Jako ilustrace nám může posloužit recenze knihy „Consumer Kids“ autora Eda Mayo publikovaná v Guardianu¹⁷. V knize je shrnuta případová studie sedmileté Sarah, která byla přes Dubit.com najata, aby jako ambasadorka značky Mattel propagovala svůj Barbie MP3 přehrávač mezi svými kamarády ve škole. Výměnou za vytoužený blýskavě růžový přehrávač má v popisu práce vytvoření fanouškovské stránky, kde bloguje o tomto produktu, pořizování fotografií ze své prodejní mise a jejich posílání na Dubit, kde jí také za její práci odměňují.

S tím, jak nám čím dál víc mobilních zařízení umožňuje nakupovat jejich prostřednictvím zboží a služby, se ocitáme v říší etiky impulzivního nakupování. Impulzivní nakupování není samo o sobě neetické. Například supermarkety nás celkem běžně vybízejí k impulzivním nákupům skrze product placement. S mobilním zařízením by ale mohly nastat nové problémy. Vezměme si například situaci, kdy by nás telefon „upomínal“, abychom koupili související produkt. Bylo by to založeno na našem „souhlasu“, takže by se nejednalo o spam. Až potud je všechno pořádku. Přinejhorším to bude trochu otravné, přinejlepším půjde o užitečné doporučení.

¹⁵ http://adage.com/digital/article?article_id=134036

¹⁶ <http://news.bbc.co.uk/1/hi/health/7760413.stm>

¹⁷ <http://www.guardian.co.uk/media/2009/jan/26/marketing-online-children-kids-underage-regulation>

Rozšířme však tuto situaci. Pokud známe konkrétní osobu/předmět, na který se dívá (na základě polohy, například pokud bude stát před autosalónem), a úvěrovou historii dané osoby (dostupné z webu), můžeme nabídnout půjčku „na jedno kliknutí“, abychom daného člověka „vtáhli“ a „povzbudili“ ho, aby si koupil auto? Právně ani technologicky tomu nic nebrání. Z morálního a etického hlediska by to však mohlo být považováno za pochybné. Je potřeba si uvědomit, že toto přesně zacílené vtažení a personalizace jsou možné díky propojení různých souborů dat.

Pokud se zaměříme na reklamu, je možné se ptát: do jaké míry diktuje reklama obsah? Je to zrádná otázka a většina médií popře, že by jejich obsah byl ovlivněn reklamou. Existují však signály, které říkají, že by tomu tak mohlo být vzhledem k omezené a reklamně založené škále obsahu. Zadavatelé reklamy například upřednostňují obsah, který má zábavní charakter, protože takový obsah diváka dostává do rozpoložení, kdy je více přístupný myšlence nakupování, než by tomu bylo v případě vážnějšího obsahu dokumentární povahy (který takový efekt nemá). Zajímavá a diskutabilní je také otázka profilů.

Za úvahu například stojí stručný popis následujícího patentu podaného společností Google (zdroj: Search engine journal)¹⁸. „Uživatelům jsou poskytovány personalizované reklamy za použití vyhledávače, který vyhledává dokumenty relevantní pro příslušný vyhledávací dotaz. Personalizace reklam probíhá na základě vyhledávacího profilu odvozeného z personalizovaných výsledků vyhledávání. Výsledky vyhledávání jsou personalizovány na základě uživatelského profilu uživatele, který zadává dotaz. Uživatelský profil popisuje zájmy uživatele a může být odvozen z celé řady zdrojů, včetně předešlých vyhledávacích dotazů, předešlých výsledků vyhledávání, vyjádřených zájmů, demografických, geografických a psychografických informací a informací o aktivitách.“

Zdá se, že by takový profil zaznamenával veškeré naše aktivity v kyberprostoru, které by byly individuálně navázány na naši osobu (aby mohly být tyto informace využity pro reklamní účely). Takový postup vyvolává obavy v souvislosti se soukromím, důvěrou a rizikem. Na druhé straně pak stojí anonymizované profily, jejichž cílem je anonymizovat osobní údaje a pak vytvořit „šablony“ uživatelského chování, které mohou být použity pro odhadování budoucího chování na základě chování v minulosti. Například by mohly pomoci předem určit, kdo odejde/ přejde jinam z konkrétní sociální sítě. V tomto případě jde spíše než o individuální profily o uživatelské segmenty. Uživatelské segmenty nejsou spojeny s jednotlivci (pochopitelně v případě velmi malého segmentu, například segmentu o jednom členovi, by se jednalo o přímé spojení).

Pokud je řeč o mobilních platformách, mají mobilní operátoři obecně dobrou pověst, co se týče správy dat a předcházení jejich zneužití reklamním průmyslem. Zavádějící promoční kampaně, jako například vyzvánění šíleného žabáka (Crazy Frog)¹⁹ v Evropě, nemají na svědomí telekomunikační operátoři, ale společnosti působící v oblasti mobilního marketingu. S jistotou se dá říci, že většina operátorů bere soukromí vážně. V průběhu času se mobilní operátoři a celé odvětví jako takové budou muset vypořádat s novými výzvami a pracovat s novými formami reklamy, jak bylo naznačeno výše. Ať zvolíme jakoukoli cestu, „mobil“ díky své jedinečné, personalizované povaze bude muset jít nad rámec „vyjádření souhlasu“ a k zajištění ochrany zájmů

¹⁸ <http://www.searchenginejournal.com/google-advertising-patents-for-behavioral-targeting-personalization-and-profiling/2311/>

¹⁹ <http://www.out-law.com/page-6483>

spotřebitelů bude pravděpodobně potřeba vyššího standardu, než jaký nabízí zákonné předpisy vycházející z představy morální a etické integrity. Budoucnost soukromí bude spočívat v posílení pozice zákazníka. Mezi mechanismy související se soukromím, jimiž se budeme zabývat později, patří:

- anonymizace;
- odvolání;
- řízení vztahu s prodejci; a
- plné zpřístupnění.

Marketéři čelí silnému pokušení přistupovat k sociálním médiím a digitální stopě jako ke „kanálu“ a podlehnout touze přizpůsobit nový svět komunikace známému světu značek, obchodního styku, cílových skupin, růstu a hodnoty. Takový přístup ale není (vždy) v zájmu spotřebitelů. Legislativní kyvadlo se přehoupne z důrazu na značky k posilování pozice spotřebitele, přičemž debata na toto téma právě začíná.

Vnímání soukromí

Je zajímavé sledovat reakci veřejnosti na otázky soukromí. Určitý vhled do vnímání zákazníků přináší Pew International²⁰. Z jejich analýzy vyplývá následující: „Dospělé, kteří se pohybují v on-line prostředí, lze rozdělit do čtyř kategorií na základě toho, do jaké míry se obávají o své on-line informace a zda se nějakým způsobem pokouší omezit svoji on-line stopu, či nikoli:

- „Sebejistí kreativci“ představují nejmenší z těchto čtyř skupin. Tvoří ji 17 % dospělých pohybujících se v on-line světě. Tvrdí, že nemají obavy v souvislosti s dostupností svých on-line dat a aktivně vystavují obsah, nicméně se také snaží omezit své osobní údaje.
- „Znepokojení a opatrní“ si dělají starosti o své osobní údaje, které jsou o nich dostupné on-line, a aktivně vyhledávají způsoby, jak omezit svá vlastní on-line data. Do této kategorie spadá každý z pěti dospělých pohybujících se v on-line prostředí (21 %).
- Přestože mají obavy z toho, kolik informací je o nich dostupných, nepodnikají členové skupiny „pasivně se obávajících“ žádné aktivní kroky, aby údaje, které jsou o nich dostupné on-line, omezili. Tuto skupinu tvoří 18 % dospělých pohybujících se v on-line prostředí.
- Skupina „neohrožených a nečinných“ je ze všech čtyř nejpočetnější – do této kategorie spadá 43 % dospělých pohybujících se v on-line prostředí. Tito uživatelé se ani neobávají o své osobní údaje, ani množství informací, které lze o nich najít on-line, nijak neomezují.“
- Z toho nám vyplývá celá škála vnímání soukromí a digitálních stop. Jak uvidíme dál, problematické oblasti, výhody a vnímání se v blízké budoucnosti značně promění, a to zejména ve vztahu k mobilním technologiím.

²⁰ <http://pewglobal.org/reports/display.php?ReportID=247>