UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Matej Poglajen

Upravljanje zasebnosti na spletnem družbenem omrežju Facebook

Diplomsko delo

Ljubljana, 2014

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Matej Poglajen

Mentor: izr. prof. dr. Gregor Petrič

Upravljanje zasebnosti na spletnem družbenem omrežju Facebook

Diplomsko delo

Ljubljana, 2014

ZAHVALA

Zahvalil bi se svojemu mentorju, dr. Gregorju Petriču, za strokovno pomoč, usmerjanje in potrpežljivost pri izdelavi diplomske naloge.

Največja zahvala pa gre moji družini: očetu Zdenku, mami Branki in bratu Damjanu, ki so mi stali ob strani, mi omogočili študij in vedno verjeli vame.

Zahvalil bi se vsem tistim, ki so me spremljali skozi študijska leta in pustili poseben pečat v mojem življenju.

Zahvala gre tudi Klavdiji Namurš in Nataliji Šraml za lektoriranje te diplomske naloge.

»Niso vsi, ki zaidejo, izgubljeni.«

(J. R. R. Tolkien)

Upravljanje zasebnosti na spletnem družbenem omrežju Facebook
Spletno družbeno omrežje Facebook je eno izmed najbolj priljubljenih in najhitreje rastočih tovrstnih spletnih servisov v svetu, ki poleg povezovanja s prijatelji in spoznavanja novih ljudi, omogoča še vrsto drugih uporabnikom relevantnih stvari. Pogostokrat se uporabniki niti ne zavedajo, da v zameno za pridobljene, pogosto navidezne koristi, Facebooku in tudi tretjim osebam posredujejo svoje osebne podatke. Zasebnost na Facebooku je zelo izpostavljena, debatirana tako v medijih kot v znanstveni srenji, saj se njeni uporabniki pogosto srečujejo s težavami pri upravljanju zasebnosti. Skozi leta so upravljavci Facebooka vnašali različne spremembe v politiko upravljanja z osebnimi podatki, da bi čim bolj ugodili uporabnikom; te spremembe so naletele na različne odzive. Ena izmed sprememb je tudi različna nastavitev zasebnosti, ki je lahko v pomoč uporabnikom, ker lahko sami nastavijo in tako določijo, kaj in v kolikšni meri želijo razkriti. V diplomskem delu želim predstaviti načine upravljanja zasebnosti, s tem pa pomagati uporabnikom pri razumevanju vidikov zasebnosti na Facebooku.

Ključne besede: spletno socialno omrežje, upravljanje zasebnosti, nastavitve zasebnosti, nadzor informacij.

The management of privacy on the social network Facebook
Social network Facebook is one of the most popular and one of the fastest growing networks worldwide, which in addition to connecting with friends and meeting new people, provides the user with a number of other fun activities. Often users do not realize that in exchange for the frequent supposed gains acquired, they transmit to Facebook and also to third parties their personal information. Privacy on Facebook is very exposed, debated both in media as in the scientific medium, because its users often encounter difficulties while managing privacy. Through the years, Facebook operators have been entering various changes within Facebook, regarding information management policies, in order to comply their users as much as possible, these changes have encountered different responses. One of the changes is also different privacy settings, which can help users manage their privacy and also determine what and how much they want to disclose. It is these settings that for some users often create some kind of illusion of control, which in turn leads to them sharing more than they would if it were not for such a setting. Other users are of the opinion that these privacy settings on Facebook do not help much in controlling the flow of information. The purpose of the thesis is to present the ways of privacy management, thereby helping users to understand the aspects of privacy on Facebook.

Keywords: online social networks management of privacy, privacy settings, control information.

KAZALO

KAZALO SLIK

1 UVOD

Živimo v eri t.i. družbenih medijev (ang. *social media)*, ki so preplavili splet, saj je vedno več spletnih mest, na katerih navadni uporabniki ustvarjajo ali označujejo vsebine, ki jih drugi uporabniki berejo, označujejo. Osebne informacije so tako postale lažje dostopne in predvsem javne zaradi dejavnosti uporabnikov. V čedalje bolj omreženem svetu je vse bolj prisotna zaskrbljenost glede varstva zasebnosti. Zasebnost je človekova temeljna pravica, vendar jo je dosti težje zagotavljati na spletu. Nove tehnologije in infrastrukture so s prodorom interneta in mobilnega računalništva hitro postale del našega vsakdana. Spletne storitve, tukaj mislimo tudi različne družbene medije, lahko danes uporabljamo preko marsikatere elektronske naprave, kar odpira nove možnosti za dostop do informacij in tudi različne možnosti upravljanja zasebnosti (Dourish in Palen 2003).

V kontekstu družbenih medijev so še posebej popularna t.i. spletna socialna omrežja (ang. *social networking sites*).Lahko bi rekli, da so nepogrešljiv del naših življenj, saj so na nek način naredila dostopnejšo in predvsem enostavnejšo komunikacijo s prijatelji ter drugimi ljudmi. Uporabnikom so tako razširila možnosti za samoizražanje in socialno interakcijo, hkrati pa ustvarila tudi precej izzivov za spletno upravljanje zasebnosti.
Spletna socialna omrežja (v nadaljevanju tudi SSO) lahko definiramo kot spletne storitve, ki omogočajo posameznikom izgradnjo javnega ali poljavnega profila znotraj omejenega sistema, povezujejo seznam drugih uporabnikov, s katerimi si delijo povezavo, in omogočajo ogled in pregled njihovega seznama stikov in drugih stikov znotraj sistema. Sama narava in poimenovanje teh povezav se lahko med socialnimi omrežji razlikuje (Boyd in Ellison 2007). »Tisto, kar naredi SSO tako edinstvena, ni to da dovolijo posameznikom spoznavati nove ljudi, temveč da omogočajo uporabnikom izoblikovati in narediti njihova socialna omrežja vidna. To lahko vodi v nastajanje novih povezav med posamezniki, ki denimo v realnem življenju ne bi bile možne.«

Vendar to pogosto ni glavni cilj SSO, saj gre pri večini večjih socialnih omrežij za primarno komuniciranje z ljudmi, ki so bili že predhodno del našega življenja, pred uporabo tovrstnih omrežij (Boyd in Ellison 2007). Velik preboj med najpopularnejša omrežja je uspel družbenemu omrežju Facebook. Od svoje ustanovitve je Facebook postal največja spletna stran z več kot 1,3 milijarde mesečno aktivnih uporabnikov po vsem svetu (Tam v Stal in Fiebert 2013; Statistic Brain 2014).

Facebook je danes množično uporabljen spletni servis, ki poleg povezovanja s prijatelji ponuja še priložnosti za grajenje socialnega kapitala, socialno oporo in samoizraznost (Debatin in drugi 2009). Kljub temu pa je prisotnih veliko študij, ki izpostavljajo in opozarjajo na kritična vprašanja povezana z zasebnostjo. Medosebno razkrivanje je namreč včasih veljajo za nekaj, kar je intimno, zasebno, Facebook pa je spremenil to dojemanje (Waters in Ackerman 2011). Od samega začetka obstoja Facebooka so se namreč pogosto pojavljale težave na področju zasebnosti. Facebook sprva ni vseboval posebnih nastavitev zasebnosti, vsa vsebina je bila privzeto vidna vsem uporabnikom (takrat samo študentom nekaterih ameriških univerz) tega socialnega omrežja. Skozi serijo sprememb so uporabnikom omogočili nastavitve za določanje tega, kaj lahko delijo s kom (Boyd in Hargittai 2010).

Vprašanja zasebnosti se izpostavljajo tudi v primeru uporabe aplikacij na socialnem omrežju, ki najpogosteje niso produkt Facebooka, temveč produkt nekih tretjih oseb (ang. *third-party*) (Egele in drugi 2012). Za Facebook bi lahko dejali, da je tipičen primer, kjer ima zasebnost antagonistično vrednost. To pomeni, da imajo uporabniki določena pričakovanja glede zaščite njihove zasebnosti, kar jim Facebook tudi do neke mere ponudi s tem, da si lahko prilagodijo nastavitve zasebnosti. Facebook pa kot korporacija gleda na dobiček, ki ga ustvarja z zbiranjem podatkov o svojih uporabnikih in prodajanju teh naprej oglaševalcem. (Netchitailova 2012). Upravljavci Facebooka so v same aplikacije vključili funkcionalnosti, ki vsakemu uporabniku omogočajo, da v omejenem obsegu določa, katere podatke bo razkril. Uporabnik ima sedaj na voljo cel nabor nastavitev zasebnosti, ki so razdeljene na kategorije in podkategorije za lažji pregled in upravljanje.

Namen diplomskega dela je predstaviti pojem upravljanja zasebnosti in na primeru spletnega socialnega omrežja Facebook prikazati, kakšne možnosti upravljanja z zasebnostjo obstajajo in kakšne so morebitne implikacije le-tega.

Cilj naloge je preučiti in predstaviti nastavitve zasebnosti na Facebooku. Za raziskovanje problema bom analiziral obstoječe znanstvene raziskave, na empirični ravni pa bo predstavljen pregled in analiza nastavitev zasebnosti.

2 ZASEBNOST

Zasebnost štejemo kot temeljno človekovo pravico, ki nima univerzalne definicije. Vsakdo ima namreč drugačna pričakovanja glede zasebnosti, te pa se spreminjajo glede na družben kontekst (Kovačič 2006). Pogosto je definirana kot »selektiven nadzor dostopa do sebe« (Altman v Cavusoglu in drugi 2013, 7). Je večplasten pojem, čigar osrednja naloga je želja po ohranitvi podatkov pred nezaželenimi posegi (Cho in drugi v Mohamed 2010). Z vidika človekovih pravic lahko zasebnost opredelimo kot pravico, da je posameznik sam in ni moten od ostalih (Wang v Al-Shakhouri in Mahmood 2009). Po Čebulju ločimo tri sestavine zasebnosti, in sicer:

- zasebnost v prostoru, ki se nanaša na posameznika in možnost, da je sam,
- zasebnost osebnosti, ki zajema svobodo misli, opredelitev in izražanj,
- informacijska zasebnost, pri kateri gre za možnost posameznika, da obdrži podatke in informacije o sebi, ker ne želi, da bi z njimi bili seznanjeni drugi (Čebulj v Kovačič 2003, 34).

Zasebnost je pomembna predvsem zato, ker ščiti svobodo posameznika, mu omogoča svobodno odločanje brez vmešavanja in prisile drugih, pri čemer je potrebno poudariti, da prisila ni nujno samo neposredna, fizična ali vidna, temveč gre lahko tukaj tudi za manipulacijo in pritiske normalizacije.

V tem primeru se zasebnost nanaša na vzpostavitev meje med posameznikom in drugimi, ki po eni strani preprečuje odtekanje informacij o posamezniku k drugim, po drugi strani pa posameznika ščiti pred zunanjimi vplivi. Mejo zasebnosti nadzoruje vsak posameznik, saj se sam odloči, katere informacije je pripravljen razkriti in pod katerimi pogoji (*Kovačič 2006*).

2.1. Zasebnost na internetu

Internet spreminja način življenja ljudi, saj jim omogoča, da z le nekaj kliki sledijo novicam, kupujejo stvari in komunicirajo z ljudmi s celega sveta. Prav tako omogoča tudi zbiranje velike količine informacij, ki jih ljudje zavedno ali nezavedno razkrivajo (Chung in Paynter 2002).

V vsakdanjem življenju puščamo za seboj sledi, odtise, na podlagi katerih lahko odkrijejo našo identiteto. Tako je tudi pri uporabi interneta, kjer puščamo tako imenovane digitalne sledi, le da običajno te ne izginejo tako hitro (Madden in drugi 2007). Spletna mesta, še posebej spletni iskalniki, zbirajo podatke, informacije in dokumente o uporabnikih, ki se nato shranjujejo v njihove strežnike (Gabor, 2013). Da je uporabnikova prisotnost na spletni strani zabeležena, poskrbijo piškotki (ang. Cookies). To so majhne tekstovne datoteke, ki jih strežnik obiskane strani namesti na uporabnikov računalnik. Piškotki vsebujejo različne informacije: od števila obiskov na spletni strani pa do uporabniških imen in gesel. Le-ti lahko predstavljajo grožnjo uporabnikovi zasebnosti na internetu predvsem iz dveh vidikov. Prvi je ta, da lahko s pomočjo piškotkov preverimo seznam obiskanih spletnih mest in pridemo tudi do osebnih informacij, ki so bile vnešene na katerem izmed spletnih mest. Drugi način, kako lahko piškotki vplivajo na uporabnikovo zasebnost, pa je ta, da je možno z njimi prepoznati IP naslov uporabnika in s tem ugotoviti natančno lokacijo računalnika, ki dostopa do strani (Zimmerman 1998). Poleg piškotkov lahko omenimo še razne parazitne, vohunske programe, kot so Spyware, ki se uporablja za prikrito zbiranje podatkov, Adware, ki je namenjen prikazovanju oglasov in prikrita omrežja, ki so omrežja računalnikov, ki si delijo določene podatke in delujejo po principu vsak z vsakim (ang. peer-to-peer). Našteti programi se običajno nezavedno namestijo na računalnik ob prenosu kakšnega programa in s tem pridobijo dostop do uporabnikove vsebine na računalniku, ki jo lahko posredujejo naprej (SI-CERT 2002).

2.2 Zasebnost pri spletnih socialnih omrežjih

Spletna socialna omrežja postajajo glavni način komuniciranja na internetu. Eksponentna rast SSO in njihove uporabe ponuja večji nabor možnosti za komunikacijo in izmenjavo informacij, obenem pa sproža številna vprašanja o zasebnosti, še posebej z upravljanjem zasebnih informacij med komunikacijo z drugimi uporabniki (Lee 2013).

Sodelovanje v spletnih socialnih omrežjih od uporabnikov zahteva delitev in razkritje osebnih podatkov (Palen v Strater in Lipford 2008). Zavedati se je potrebno, da se lahko uporabniki zaradi razkritja osebnih podatkov soočajo tudi z neprijetnimi situacijami, izsiljevanjem ali celo krajo identitete (Strater in Lipford 2008). Informacije, ki se izmenjujejo preko socialnih omrežij, potujejo veliko hitreje kot v realnem življenju.

SSO so sestavljena iz uporabniških računov in povezav med uporabniki. Nekatera omogočajo uporabnikom, da se povežejo z drugimi uporabniki brez njihovega soglasja, medtem ko druga zahtevajo soglasje obeh uporabnikov, preden se ustvari povezava med njima. Uporabniki med seboj tvorijo povezave iz številnih razlogov. Eden je ta, da ustvarjena povezava znotraj spletnega omrežja odraža tudi povezavo v realnem življenju, lahko gre tudi za skupne interese ali poslovne stike (Mislove in drugi 2007). Pri ustvarjenih povezavah zelo pogosto govorimo o prijateljstvu in prijateljih, ki pa ne predstavljajo nujno tesnih vezi med uporabniki, ki so prisotne pri dejanskem prijateljstvu v realnosti. Prijateljstvo je na spletnih socialnih omrežjih po besedah Boydove, funkcija, ki potrjuje povezavo med uporabniki in jim omogoča artikulacijo svojega namišljenega občinstva ali izbrane skupine ljudi, za katere se jim zdi, da so del njihovega sveta v mejah spletnega mesta (Boyd v Ellison in Boyd 2007, 2013).

Stanja, fotografije, videoposnetki so privzeto vidni vsem uporabnikom socialnega omrežja. Uporabniki, ki se zavedajo vprašanj zasebnosti in znajo upravljati z nastavitvami zasebnosti, pa lahko omejijo vidnost na določene skupine ljudi (Cutillo in drugi 2009). Medtem ko je upravljanje identitete in zasebnosti kontinuiran, dogovorjen proces pri medosebnem komuniciranju, je proces odločanja pri računalniško posredovanem komuniciranju nekoliko težji. Uporabniki so poredko v sinhroni interakciji med seboj, tako da se morajo vnaprej in jasno odločiti, kaj bodo drugim razkrili (Strater in Lipford 2008). Pri tovrstnih odločitvah pomagajo posamezne nastavitve in mehanizmi SSO. Ena izmed njihovih nalog je določitev, kdo ima dostop do naših informacij in komu preprečimo ogled nekaterih vsebin na profilu.

Čeprav večina omrežij omogoča uporabnikom, da sami nadzorujejo, kaj deliti s kom, je njihovo politiko nadzornega dostopa težko razumeti in ustrezno nastaviti. Tukaj se poraja vprašanje, ali nastavitve zasebnosti spletnih družbenih omrežij ustrezajo uporabnikovim delitvenim nameram (Madejski in drugi 2011). Kljub temu da je večina spletnih družbenih omrežij pogosto kritiziranih ravno zaradi pomanjkanja pozornosti in skrbi za zasebnost njihovih uporabnikov, te platforme še zmeraj najdejo pot do novih uporabnikov (Cavusoglu 2013).

Pri SSO se uporabniki srečujejo z različnimi tveganji, povezanimi z zasebnostjo, ki pa jih lahko razdelimo v tri kategorije:

Varnost: Zaradi velikega pretoka osebnih informacij na spletnih socialnih omrežjih, so lahko uporabniki izpostavljeni številnim spletnim napadom, kot so kraja identitete, spletno nadlegovanje, spletno ribarjenje (ang. phishing), podtikanje zlonamernih programov (ang. malware) (Ho 2012, 23).

Ugled in verodostojnost: Ugled lahko definiramo kot družbeno oceno javnosti do osebe, skupine ali organizacije. Na SSO mora uporabnik paziti na svoj ugled, saj lahko vpliva na njegovo verodostojnost v resničnem življenju. Veliko delodajalcev namreč preverja spletne profile potencialnih zaposlenih in se lahko na videno vsebino odločijo, če jim bodo ponudili delo (Ho 2012, 23-24).

Profiliranje: običajno gre za zbiranje metapodatkov, kot tudi osebnih in vsebinskih podatkov o nekem uporabniku. Mnoga podjetja in upravljalci spletnih mest zbirajo podatke iz večih virov, za izgradnjo celovitih profilov za posameznike, na podlagi katerih bi nato prodajali izdelke. SSO si dobiček ustvarjajo z oglaševanjem, tako da jim podjetja plačujejo, v zameno pa njihove oglase prikazujejo vsem, ki bi jih vsebina zanimala. Tako uporabniki običajno zasledijo individualno »krojene« oglase, ki so zasnovani na podlagi vsebine iz uporabniških profilov. Zbiranje teh podatkov običajno poteka brez soglasja osebe, kateri je profiliran izdelek ponujen. Čeprav zbiranje javno dostopnih podatkov ni nelegalno, pa uporabniki SSO nimajo nadzora, kako bodo ti podatki uporabljeni (Ho 2012, 25–26).

Izpostavimo lahko dva pogosta dejavnika, ki lahko privedeta do omenjenih tveganj, in sicer se pogosto zgodi, da uporabnikov ne skrbi razkritje osebnih informacij in tako niti ne posvečajo pozornosti nastavitvam zasebnosti. Druga skupina uporabnikov pa je, kot smo že omenili, seznanjena s tveganji, a zaradi kompleksnosti ali nerazumevanja nastavitev ne uspejo nastaviti ustrezne zaščite (Das 2014).

3 UPRAVLJANJE ZASEBNOSTI

»Znotraj »offline« socialnih prostorov, predstavlja upravljanje zasebnosti del vsakdanjega življenja, ki vpliva na odločitve kje, kdaj in komu bomo razkrili osebne podatke.« (Dwyer in drugi 2010). V čedalje bolj omreženem svetu skrb za zasebnost predstavlja pogost problem. Vse nove tehnologije in infrastrukture, ki se pojavljajo v vsakdanjem življenju, prinašajo s seboj nove možnosti za dostop do informacij, kot tudi za upravljanje zasebnosti (Palen in Dourish 2003). »Upravljanje zasebnosti opredeljuje načine, na katere posamezniki in organizacije nadzorujejo zbiranje, uporabo in izmenjavo osebnih podatkov, vključno z občutljivimi informacijami« (Pearson in Mont 2011). Pri tem ne gre zgolj na določanje pravil in njihovo uveljavljanje, pač pa za stalno upravljanje mej med različnimi področji delovanja in stopenj razkritja na teh področjih (Palen in Dourish 2003). Upravljanje zasebnosti velja za eno izmed bistvenih socialnih veščin, ki jih najdemo v različnih kulturah povsod po svetu. Sestoji iz različnih komponent, kot so socialna, relacijska, kognitivna in zaznavna, ki jih uporabnik nenehno nadzoruje v realnem času. Socialna komponenta se smatra kot sposobnost za vzpostavljanje in ohranjanje interakcije in komunikacije z drugimi ljudmi v socialnem okolju, relacijska kot način, na katerega sta dve (ali več) osebi oziroma stvari povezani. Kognitivna komponenta zajema sposobnost posameznika da zaznava in dojema realnost, zaznavna komponenta pa se nanaša na čutno zaznavo sveta okoli nas, skozi katero pridobivamo informacije o stvareh iz okolja, ki jih lahko interpretiramo. Z omenjenimi komponentami posameznik nadzira razvoj meja zasebnosti in razkritje osebnih podatkov (Petronio v Dwyer in drugi 2010).

Ljudje se danes vse bolj poslužujejo različnih komunikacijskih orodij, ki temelijo na internetu in sami prispevajo k vsebini, ki jo najdemo na spletu. Uporaba je preprosta in na voljo je širok spekter spletnih strani za ogled fotografij in videoposnetkov, za povezovanje, pisanje blogov in podobno. Večina teh strani je zasnovanih tako, da se informacije delijo hitro in enostavno, uporabniki pa za to ne potrebujejo veliko tehničnega znanja. »Vse več strani je namenjenih uporabnikovi samopredstavitvi, ki je proces, kako posameznika vidijo, dojemajo drugi ljudje. Za potrebe samopredstavitve mora uporabnik na strani zagotoviti čim več informacij o sebi.« (Leary v Rui in Stefanone 2012, 110)

Ob teh trendih se pogosto pojavljajo vprašanja zasebnosti ter kako se zavarovati pred razkrivanjem osebnih informacij (Madejski in drugi 2012). »Upravljanje zasebnosti na spletu predstavlja izzive predvsem uporabnikom SSO, ker je kognitivno zapleteno, saj je potrebno posledice razkritja informacij obravnavati glede na čas in prostor«(Dwyer 2008). SSO so zasnovana tako, da posnemajo osebne interakcije, kar privede do tega, da so uporabniki pogosto pripravljeni razkriti več zasebnih podrobnosti, kot bi jih sicer (Gross in Acquisti 2005). Nastavitve za nastavljanje zasebnosti pri SSO temeljijo na nadzoru dostopa in zahtevajo od

uporabnikov, da bodisi dovolijo ali zavrnejo dostop do njihove vsebine (Mondal in drugi 2014). Običajno se uporabljajo z namenom preprečitve razkritja informacij, ki se uporabljajo za potrebe samopredstavitve, žal pa vedno ne uspejo zagotoviti zasebnosti, saj je znotraj SSO veliko zasebnostnih mehanizmov za nadzor nad interakcijo in izmenjavo informacij prešibkih. Uspešnost uporabnikov pri upravljanju zasebnosti poleg tega ovirata tudi omejena razumnost in motivacija za nadzor nad njihovo zasebnostjo (Wisniewski in drugi 2014; Govani in Pashley 2005).

Preden nadaljujemo s poglavjem o spletnem socialnem omrežju Facebook, še na kratko omenimo teorijo komunikacijske zasebnosti, ki predstavlja teoretski okvir, potreben za razumevanje mehanizmov za upravljanje zasebnosti in načinov, s katerimi uporabniki dosežejo ravnovesje med razkritjem in prikritjem osebnih podatkov znotraj in zunaj SSO (Catlett 2007).

Teorija komunikacijske zasebnosti ponuja sistem za upravljanje zasebnosti, ki določa, kako so postavljene meje zasebnosti pri posameznikih in med njimi (Petronio v Waters in Ackerman 2011). Meje zasebnosti omogočajo, da ljudje označijo, kdo ima nadzor nad informacijami, kdo ima oziroma nima dostopa do njih ter kako bi naj bile le-te znotraj mej zaščitene pred tistimi izven meja (Petronio in drugi v Catlett 2007). Omenjena teorija obravnava zasebnost kot občutek posameznika, da si ima pravico lastiti zasebne podatke, tako osebno kot kolektivno (Petronio v Waters in Ackerman 2011). Teorija poudarja tudi, da je potrebno preučiti komunikativne interakcije med ljudmi, da bi razumeli mehanizme upravljanja zasebnih podatkov. Ideja teorije je, da imajo ljudje željo po zasebnosti in dinamični procesi razkrivanja in prikrivanja zasebnih podatkov predstavljajo proces, ki izpolnjuje to željo (Lee 2013). Upravljanje zasebnosti se tako nanaša na procese, kako ljudje vsak dan sprejemajo odločitve, koliko informacij so pripravljeni razkriti drugim in koliko jih bodo ohranili zase. Omeniti velja tudi pet temeljnih principov (v Petronio 2002) te teorije, ki se jih da aplicirati na nekatera SSO:

1) Z upravljanjem zasebnosti sami določamo svoje meje zasebnosti, saj predpostavljamo, da imamo nadzor in lastništvo nad našimi zasebnimi informacijami.
2) Sami določamo, komu je dovoljen dostop do zasebnih informacij, katere nadziramo z uporabo osebnih zasebnostnih pravil.
3) Ko nekdo pridobi dostop do naših zasebnih informacij, s tem postane »solastnik« teh informacij.
4) Solastniki zasebnih informacij se morajo dogovoriti o zasebnostnih pravilih, ki veljajo za oba.
5) V kolikor ne pride do dogovora o zasebnostnih pravilih, lahko pride do »turbolence«

Te principe bomo v nadaljevanju aplicirali tudi na Facebook, ko bomo govorili o upravljanju zasebnosti.

4 SPLETNO SOCIALNO OMREŽJE FACEBOOK

»Študentsko življenje brez Facebooka je skoraj nepredstavljivo. Od njegove uvedbe leta 2004 je to popularno spletno družbeno omrežje hitro postalo ne samo osnovno orodje, ampak tudi ogledalo družbene interakcije, osebne identitete in grajenja omrežij med študenti« (Debatin in drugi 2009).

Pri Facebooku so svoje spletno socialno omrežje definirali kot družbeni pripomoček, ki pomaga ljudem pri bolj učinkoviti komunikaciji s svojimi prijatelji, družino in sodelavci. Njihova naloga je dati ljudem pravico, da lahko delijo vsebino z drugimi in s tem naredijo svet bolj odprt in povezan. Pri Facebooku razvijajo tehnologije, ki omogočajo izmenjavo informacij prek socialnega grafa, ki je odsev resničnih družbenih povezav med ljudmi. Gre za zaupanja vredno okolje, kamor se lahko vsak prijavi in komunicira z ljudmi, ki jih pozna (Waters in Ackerman 2011; Facebook 2014).

Za pridružitev k Facebooku je potrebno navesti svoje ime in priimek, elektronski naslov, spol in rojstni datum. Rojstni datum je pomemben, saj velja starostna omejitev, ki prepoveduje uporabo mlajšim od 13 let. Po uspešni registraciji nas čakajo številni koraki, od iskanja svojih prijateljev, izpolnjevanja profila, kjer lahko navedemo informacije o kraju bivanja in rojstva, šolanju in delodajalcu. Zadnji korak je nastavitev prikazne fotografije in s potrditvijo postanemo uradni člani SSO Facebook.

Facebook se je že v samem začetku delovanja nekoliko razlikoval od ostalih, takrat obstoječih spletnih socialnih omrežij, saj se mu je lahko priključila izključno izbrana populacija – študenti Harvardske univerze v ZDA. Postopoma so se razvili koncepti omrežij, tako da so se lahko priključile tudi ostale univerze. V letu 2006 pa je Facebook postal dostopen vsem in je do sedaj postal mednarodna mreža, ki presega več kot milijardo aktivnih mesečnih uporabnikov (Boyd in Hargittai 2010; Constantine v Blank in drugi 2014).

Obravnavano spletno socialno omrežje sestoji iz različnih segmentov, ki sestavljajo celoto Facebooka (Das 2014). Izpostaviti velja naslednje:

Uporabniški profil: je vizualna predstavitev in prikaz osebnih podatkov, povezanih z določeno osebo.

Zid ali časovnica: gre za kombinacijo uporabnikovega zidu in profila v enem. Leta 2011 so pri Facebooku z uvedbo časovnice drastično spremenili obliko in način postavitve profilov.

Časovnica je tako postala zbirka fotografij, objav in izkušenj, ki pripovedujejo uporabnikovo zgodbo (Facebook 2014). Uporabnikova vsebina je organizirana v kronološkem zaporedju, ki temelji na datumu objave (Stal in Fiebert 2013). Z uvedbo časovnice se je spremenila tudi orodna vrstica, ki je sedaj bolj konsistentna in enostavnejša za uporabo na različnih platformah.

Zbirnik novic: imenujemo ga tudi domača stran, ki se prikaže, ko se uporabnik prijavi na Facebook. Zbirnik novic prikazuje, posodobitve, objave, prihajajoče dogodke in rojstne dneve uporabnikovih FB prijateljev. Med novicami se vse pogosteje pojavljajo tudi sponzorirani oglasi in predlogi strani, ki bi naj zanimale uporabnika.

Prijatelji: pojem se nanaša na vsako osebo, ki je na Facebooku povezana z uporabnikom in je vidna na njegovem seznamu prijateljev. Prijateljstvo nastane, ko ena oseba pošlje drugi prošnjo, ta druga oseba pa mora prošnjo potrditi. Prošnjo za prijateljstvo je možno tudi zavrniti, kar pa ne prepreči prosilcu, da je čez čas ne pošlje ponovno.

4.1 Upravljanje zasebnosti na Facebooku

»Medosebno razkritje podatkov je bilo nekoč nekaj, kar je potekalo v intimni in zasebni sferi, toda Facebook je spremenil to zaznavanje« (Waters in Ackerman 2011, 101). Nastavitve na Facebooku so privzeto nastavljene, da se uporabnikova vsebina deli z drugimi uporabniki omrežja. Uporabnik ima nadzor in možnosti izbire pri tem, kakšen vtis bo pustil pri drugih, kar je lahko precej zahtevno. Poiskati je potrebno ravnotežje med javno vsebino in tisto bolj zasebne narave, za katero je iz številnih razlogov (zloraba podatkov, kraja identitete, nadlegovanje in podobno) bolje, da se ne deli z ostalimi. Čeprav se uporabnik svobodno odloča kaj in na kakšen način bo delil z ostalimi, pa nima vedno popolnega nadzora nad vsebino, ki jo lahko drugi razkrijejo o njemu (npr. oznaka uporabnika v objavi, na fotografijah in podobno)(Lampinen in drugi 2011). Svojo vsebino in vsebino, ki se direktno navezuje na uporabnika, lahko upravlja s pomočjo nabora nastavitev zasebnosti, ki se jim bomo posvetili v nadaljevanju naloge.

Spletno socialno omrežje Facebook je skozi čas doživelo veliko sprememb tudi na področju upravljanja vsebine. Na začetku je bila vsa vsebina, kot smo že omenili, vidna zgolj osebam znotraj istega omrežja (univerze v ZDA), skozi vrsto preoblikovanj, ki so sledila, pa je Facebook uporabnikom omogočil nadzor nad tem, kaj lahko delijo in s kom. Za vsako objavo so bile na voljo različne možnosti, komu bo vsebina vidna (»prijatelji«, »prijatelji prijateljev«, »po meri«). Kasneje, ko se je Facebook razširil, so ga množično začela uporabljati razna podjetja, ki so ustvarjala spletne aplikacije in Facebook je pričel s projektom »Facebook Platform«, ki je

zagotavljal okvir za razvijalce programske opreme za razvijanje aplikacij, ki so tekle na spletnem socialnem omrežju (developers.facebook). Aplikacije so pogosto povzročile, da se je uporabnikova vsebina delila z zunanjimi razvijalci (ang. Third-party), saj so ustvarjene aplikacije za delovanje potrebovale nekatere osebne podatke. Posledično so bile uvedene nove nastavitve zasebnosti, ki omogočajo uporabnikom, da določijo, kateri izmed tretjih oseb dovolijo dostop do katerih vsebin. Sporočila za tovrstne nastavitve se prikažejo vsakič, ko se uporabnik prvič odloči za uporabo aplikacij (Boyd in Hargittai 2010).

Nastavitve zasebnosti so se vseskozi nekoliko izpopolnjevale in kontrole so postale vse bolj zapletene (Boyd in Hargittai 2010). Zapletene in nenehno spreminjajoče se politike zasebnosti na spletni strani zahtevajo od uporabnikov, da so izredno pozorni na njene posodobitve, da bi ohranili zavedanje o nastavitvah zasebnosti. Kadar se posamezniki ne zavedajo teh nastavitev, lahko postanejo vsebine in osebni podatki, ki jih objavijo, dostopni širšem krogu občinstva, kot je bilo sprva namenjeno. Ta pojav je zlasti kritičen v času, ko je Facebook postal ena izmed najpogostejših oblik dnevne komunikacije (Butler in drugi 2011). Zaradi negotovosti uporabnikov, kaj katera sprememba v nastavitvah sploh povzroči, so pri Facebooku sčasoma poenostavili nastavitve zasebnosti (Zuckerberg v Boyd in Hargittai 2010). Te spremembe so povzročile številne kritike, saj so bile videti kot poskusi, da bi omajali zasebnost uporabnikov in tako postopno znižali pričakovanja glede zasebnosti (Anderson v Cavusoglu in drugi 2013).

Ljudje imajo ob pridružitvi k Facebooku prepričanje, da si lastijo svoje zasebne informacije in imajo pravico do nadzora le teh. Do neke mere to drži, toda običajno uporabnik ob registraciji ne premišljuje veliko. Poda potrebne osnovne podatke, kot so ime in priimek, rojstne podatke in veljaven elektronski naslov. Drugi podatki, ki smo jih omenili že v poglavju o Facebooku, niso obvezni in jih uporabnik izpolni po želji. V kolikor jih izpolni, so ti podatki vidni na njegovem profilu in si jih lahko, (v kolikor nima ustrezno nastavljenih nastavitev zasebnosti), ogleda vsak uporabnik Facebooka. Z nastavitvami zasebnosti lahko vsak uporabnik nadzira svoje zasebne informacije Na voljo ima različne, prednastavljene možnosti za nastavitev vidnosti profila, lahko pa si tudi sam prilagodi nastavitve. Če se spomnimo drugega temeljnega principa upravljanja komunikacijske zasebnosti, da lahko ljudje nadzirajo svoje zasebne informacije z uporabo osebnih zasebnostnih pravil, potem lahko vidimo, da Facebook to uporabnikom omogoča. Težava je v tem, da mnogi uporabniki tem nastavitvam ne posvečajo dovolj pozornosti, kar lahko privede do razkritja podatkov. Vidni podatki na profilih uporabnikov so tako dostopni tudi FB-ovim prijateljem ali celo vsem uporabnikom, če ni drugače nastavljeno. Tukaj se srečamo s tretjim principom, da ko pride oseba do informacij druge osebe, postane s tem solastnik informacije. Uporabnikov prijatelj na FB-u lahko na profilu vidi različne informacije, in če bi se zgledovali po četrtem principu, bi morala solastnika med seboj skleniti zasebnostna pravila, kar pa na Facebooku ni v navadi, saj se predpostavlja, da solastnik informacij ne bo širil naprej. V

kolikor se te predpostavke ne upošteva in nekdo uporabi ali posreduje zasebno informacijo tretji osebi, pride do pete predpostavke, turbolence, rezultat te pa je ponavadi nezaupanje, jeza ali nesigurnost »oškodovanega« uporabnika.

4.2 Aplikacije in Facebook

Ena izmed ključnih točk, ki so privedle Facebook do tako velikega uspeha in priljubljenosti, je nedvomno njegova aplikacijska platforma, ki omogoča razvoj aplikacij s strani tretjih oseb (Gjoka in drugi 2008). »Facebook Platforma zajema nabor vmesnikov (npr. API) in storitev, ki omogočajo drugim, vključno z razvijalci aplikacij, da pridobijo podatke iz Facebooka ali jih posredujejo« (Facebook 2014).

Aplikacija je vrsta programske opreme, ki omogoča opravljanje posebnih nalog in je namenjena končnim uporabnikom – osebam, ki jo bodo uporabljale. Aplikacije običajno razvijajo ponudniki operacijskih sistemov in druge programske opreme. V primeru ko aplikacija ni produkt ponudnikov storitev, temveč posameznikov ali podjetij, ki so neodvisni od primarnega produkta, gre za aplikacije tretjih oseb (Kayne in Wallace 2014).

Facebook aplikacije

Pri Facebooku so v letu 2007, v želji po izboljšanju uporabniške izkušnje, uvedli platformo za razvijalce, ki so lahko začeli ustvarjati različne aplikacije za bogatenje Facebookove funkcionalnosti. Facebookov aplikacijski model je edinstven, saj je tveganje pri razvoju in promoviranju aplikacij tretjih oseb veliko manjše kot pri vlaganju v samostojne spletne aplikacije (Gjoka in drugi 2008). Z uporabo aplikacij pa se pojavljajo tudi nekatere polemike glede zasebnosti. Neodvisni razvijalci aplikacij imajo namreč dostop do knjižnic v aplikacijski platformi, preko katerih je možno dostopati tudi do osebnih podatkov Facebookovih uporabnikov. Na primer, če aplikacija za dostop potrebuje uporabnikove podatke, bo ustrezen vnos v knjižnico vrnil to vrednost. Vse komunikacije, ki se zgodijo med aplikacijo in družbenim omrežjem, so vdelane v knjižnici. Ko aplikacija enkrat pridobi dostop do podatkov uporabnika, upravljavci spletnega socialnega omrežja ne morejo oceniti, kako bodo ti podatki obdelani s strani aplikacije. Zaradi pomanjkanja tehničnih sredstev so zato pri Facebooku uvedli zahtevo, da se razvijalci aplikacij strinjajo z njihovimi pogoji storitev, ki med drugim navajajo, da aplikacije ne smejo hraniti zbranih podatkov uporabnikov, prav tako ne smejo teh podatkov širiti naprej. Kljub temu je bilo že veliko prijav glede kršitev teh pogojev. Pogosto se je zgodilo, da so razvijalci aplikacij

pridobljene podatke predali naprej oglaševalcem in podjetjem za internetno sledenje. Takšni in podobni primeri so privedli do poostritve nastavitev zasebnosti za omejevanje in nadzor dostopa aplikacij tretjih oseb do podatkov pridobljenih iz uporabniških profilov (Egele in drugi 2012).

Aplikacije, ki jih uporabnik želi zagnati, imajo poleg njihove predstavitve zapisane tudi pogoje uporabe in pravilnik o zasebnosti, tako da je uporabnik do neke mere seznanjen s tem, katere podatke bo aplikacija dobila. Običajno gre tukaj za osnovne podatke, ki so javno vidni, poleg tega pa aplikacija pridobi tudi seznam prijateljev, elektronski naslov in rojstne podatke. Uporabnik pri tem nima možnosti, da selektivno sprejme ali zavrne kaj od navedenega. Pri Facebooku navajajo, da v kolikor aplikacija potrebuje kakšne dodatne informacije, bo le-ta uporabnika prosila za posebno dovoljenje za pridobitev le-teh (Facebook 2014). Pri uporabi aplikacij velja izredna previdnost, saj je možno, da je katera izmed njih zlonamerna.

Na Facebooku najdemo različne aplikacije, veliko pozornosti pa uporabniki namenjajo predvsem igram. Aplikacije so uporabnikom na voljo brezplačno, veliko izmed njih pa ima tudi dodatne, plačljive storitve, ki uporabnikom omogočajo nakup dodatnih funkcij ali virtualnega denarja. Da lahko igramo, potrebuje aplikacija naše osnovne podatke (ime, profilna fotografija, spol, seznam prijateljev in ostale informacije, ki so nastavljene kot javne) in elektronski naslov. Aplikacija lahko tudi v našem imenu objavlja naše dosežke, ki bodo prikazani našim Facebook prijateljem.

Facebook API

Facebook API (Application Programming Interface) je platforma za gradnjo aplikacij, ki so na voljo uporabnikom Facebooka. API omogoča uporabo socialnih povezav in profilnih podatkov, za izboljšanje aplikacij in objavo dejavnosti na zbirniku novic, ki pa so odvisne od uporabnikovih nastavitev zasebnosti. Znotraj Facebooka teče več programskih vmesnikov, pomembno je izpostaviti Graph API, ki je jedro platforme in skrbi za branje in pisanje v Facebookov socialni graf, ki zajema uporabnike, fotografije, dogodke, strani in vse povezave med njimi, kot so oznake prijateljstva, oznake fotografij, deljene vsebine in druge naloge, ki naj bi jih aplikacije opravljale (developers.facebook). Obstajajo tudi Ads API, ki omogoča dostop in ustvarjanje oglasov in Pages API, ki se uporablja za ustvarjanje »fan« strani, ki jih lahko drugi uporabniki »všečkajo«, nato so tu še Public Feed API, ki zagotavlja pretok uporabnikovih posodobitev stanj, Keyword Insights API za iskanje med objavami po ključnih besedah in Chat API, ki podpira Facebook klepet na namizju ali mobilnih napravah (developers.facebook).

5 ANALIZA NASTAVITEV ZASEBNOSTI PRI FACEBOOKU

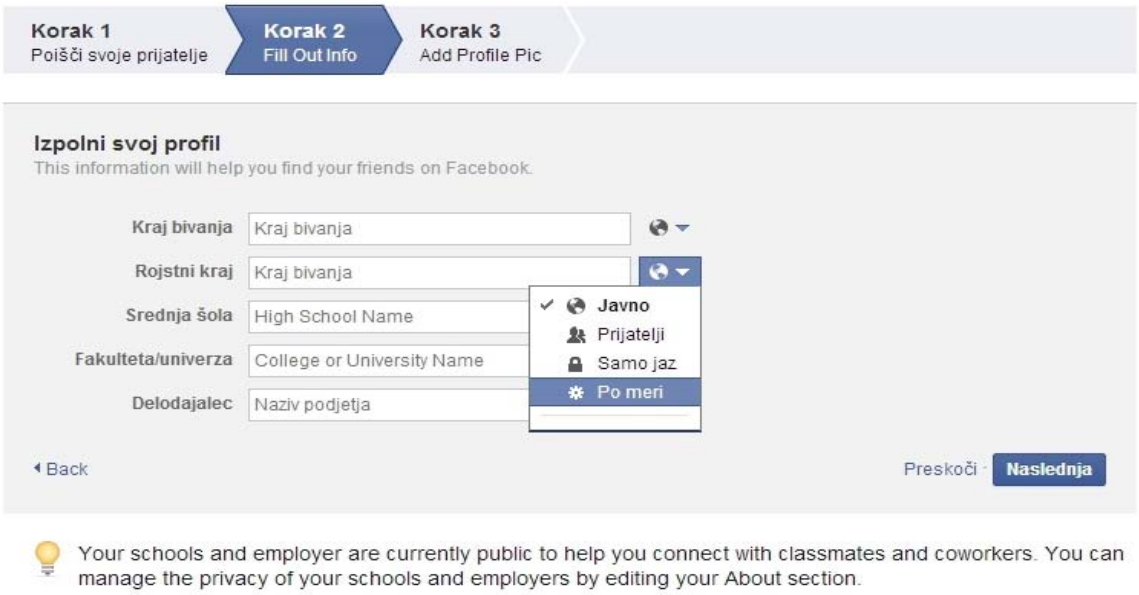
Osredotočili se bomo na nastavitve zasebnosti, ki so trenutno na voljo uporabnikom, in razložili možnosti, ki jih ponuja Facebook za upravljanje le-teh. Facebook ima številne funkcionalnosti, ki se lahko uporabijo za segmentiranje občinstva ter omejitve vidnosti informacij (Boyd in Marvick 2011). Kljub vsem različnim nastavitvam, ki omogočajo zasebnost, se jih večina uporabnikov ne poslužuje. Razlog je v tem, da imajo nekateri pogosto težave z razumevanjem upravljanja zasebnosti in tako kljub nekaterim napravljenim spremembam v nastavitvah, te spremembe ne odražajo želenega rezultata (Lipford in drugi 2008).

Pri razumevanju zasebnosti na Facebooku je uporabnikom v pomoč pravilnik o zasebnosti, ki navaja, na kakšen način so varovane in uporabljene njihove informacije in kdo lahko do njih dostopa. Žal se zaradi obširnosti tovrstnih pravilnikov uporabniki poredko odločajo za njihovo branje (O'Brien in Torres 2012). Pri nastavitvah zasebnosti lahko običajno postavimo dve merljivi spremenljivki, in sicer občutljivost in vidnost podatkov. Občutljivost podatkov se nanaša na podatke, ki so zasebne narave in ob morebitnem razkritju lahko povzročijo zadrego in neprijetnosti, vidnost pa na to, kako javni bi postali podatki ob razkritju. Merili lahko ponazorimo na konkretnem primeru nastavitev, kjer ima nastavitev, komu bodo vidne naše prihodnje objave, potencialno visoko stopnjo vidnosti, medtem ko ima nastavitev, ali želimo deliti svoje osebne podatke z aplikacijami, visoko stopnjo občutljivosti (Minkus in Memon 2014). V nadaljevanju bomo spoznali nastavitve zasebnosti, kakšen je njihov namen in kako se jih uporablja.

5.1 Prva pridružitev Facebooku

Izvedli smo celoten postopek registracije na Facebook in pregledali, kako se uporabnika seznani z nastavitvami zasebnosti in kaj lahko omeji, še preden zaključi vse korake za pridružitev. Opazimo (slika 5.1), da lahko profilnim podatkom (razen imena in priimka) omejimo vidnost. Na voljo imamo tri osnovne možnosti in četrto, ki jo nastavimo po meri. Ta zadnja možnost na samem začetku še ne igra pomena, če nimamo FB prijateljev, da bi komu izmed njih omejili dostop do informacij.

Slika 5. 1: Prikaz zasebnostnih možnosti pri prvem vnašanju informacij



Vir: Facebook (2014).

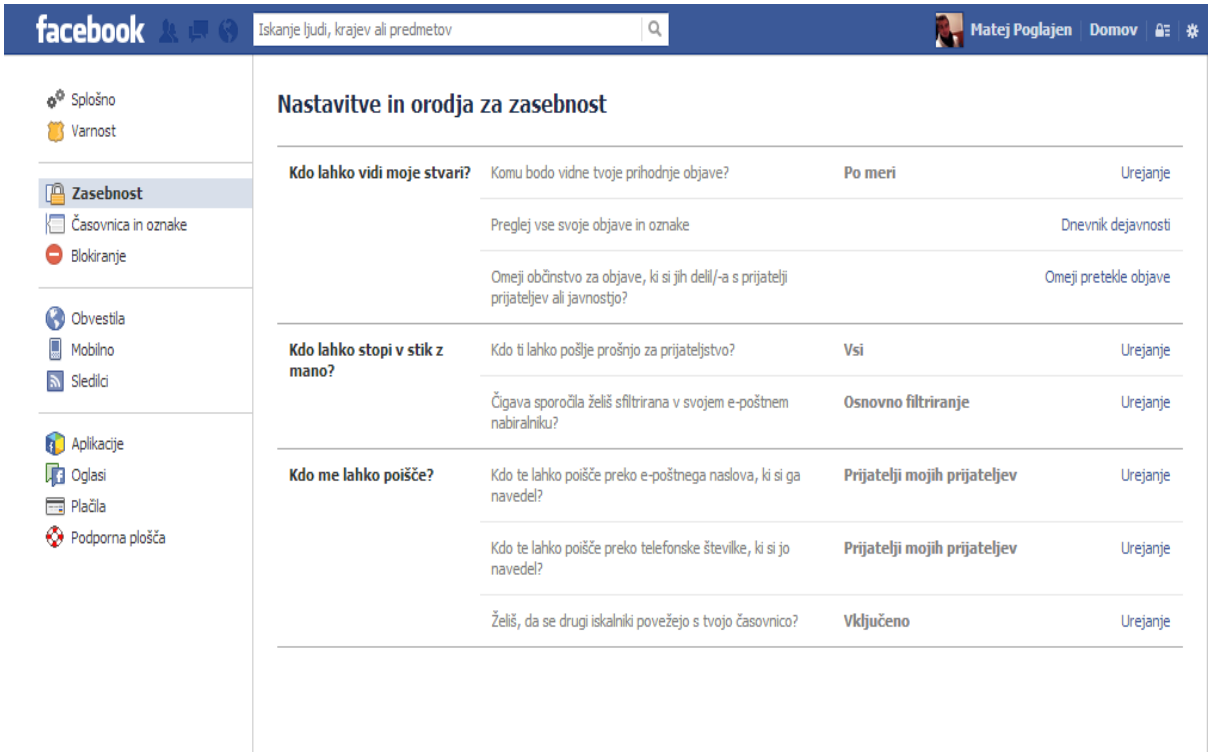
Pri tretjem koraku imamo možnost izbire profilne fotografije, ki je poleg naslovne fotografije (ang. cover photo) javna in ji ne moremo spreminjati nastavitev dostopa. Po zaključenih treh korakih smo uradno postali člani Facebooka. Stran nas povabi, da izpolnimo korake, ki smo jih prej morebiti preskočili in svetuje, da izvemo nekaj več o naših nastavitvah zasebnosti skozi štiri vodene korake. Tako izvemo, kako si nastavljamo občinstvo, s katerim bomo delili vsebino, kako deluje označevanje, kje se nahajajo zasebnostne bližnjice in kako upravljamo z aplikacijami. Vsi ti omenjeni koraki nam lahko zelo pomagajo pri nadaljnem upravljanju zasebnosti, če smo le dovolj motivirani, da preučimo vsak korak. Pred uporabo je pametno prebrati tudi politiko uporabe podatkov, za boljše razumevanje Facebookove politike. V eni izmed številnih točk izvemo, da kot uporabniki dajemo Facebooku dovoljenje, da uporablja naše registracijske informacije, informacije, ki jih sami delimo, kot tudi tiste informacije, ki jih drugi delijo o nas (npr. oznake). Ob vsaki uporabnikovi aktivnosti, kot je nalaganje fotografij ali video posnetkov, lahko Facebook pridobi tudi metapodatke, kot so čas in datum, ko je bila fotografija ali video ustvarjen. Na podlagi teh pridobljenih podatkov nam lahko Facebook ponudi različne storitve, predloge za prijateljstva.

5.2 Nastavitve in orodja za zasebnost

Uporabniki lahko spreminjajo nastavitve zasebnosti s klikom na ikono ključavnice na zgornji desni strani orodne vrstice, ki je v bistvu zasebnostna bližnjica, ki omogoča uporabniku, da na hitro pregleda svoje nastavitve in jih po potrebi tudi spremeni. Za podroben pregled nastavitev zasebnosti se uporablja ikona zobnika, ki privede uporabnika do več nastavitev. Uporabnikom so

ponujene tri glavne kategorije, ki so razdeljene na podkategorije (slika 5.2), dotaknili pa se bomo tudi nekaterih drugih kategorij, ki se navezujejo na zasebnost.

Slika 5. 2: Nastavitve in orodja za zasebnost



Vir: Facebook (2014).

Nastavitev vidnosti objav

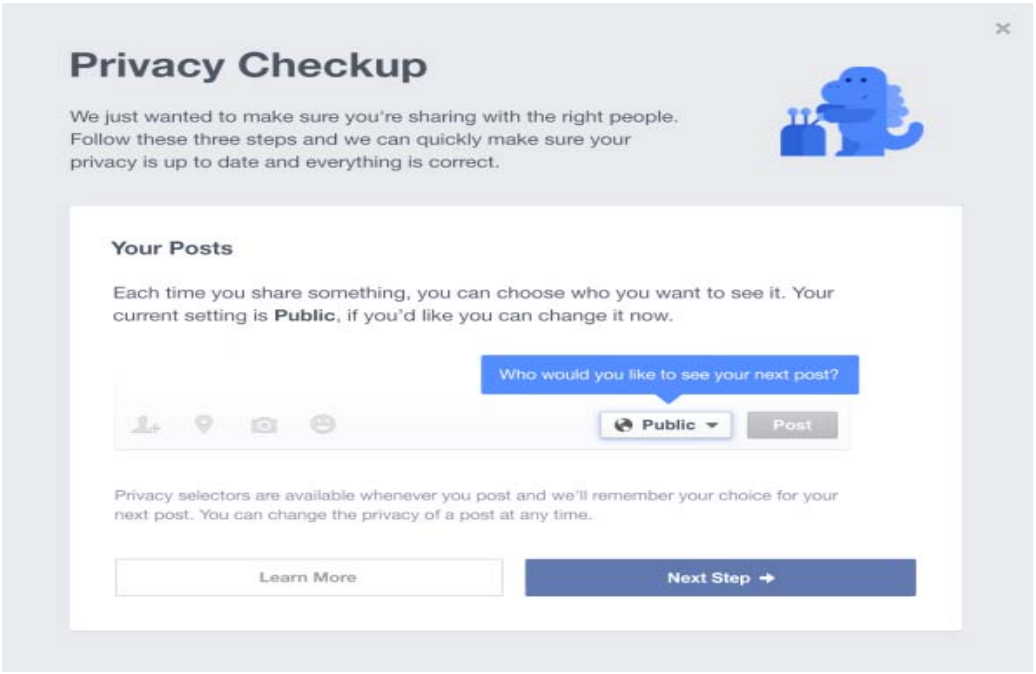
»Kdo lahko vidi moje stvari?« je možnost, kjer nastavimo, s kom želimo deliti naše objave in oznake. Dodajanje oznak v objave je postalo zelo priljubljeno. Dodamo jih lahko kamor koli, v objavo, na fotografijo, videoposnetek. Z oznako (ang. tag) običajno označimo osebo ali stvar, ki se v objavi obarva modro in postane hiperpovezava, ki preusmeri na stran označene osebe ali stvari.

Vidnost objav in oznak lahko nastavimo na »javno«, kar pomeni, da so objave vidne vsem uporabnikom, ne le FB prijateljem. Če ne želimo deliti svojih objav z vsemi uporabniki, izberemo možnost »vidno prijateljem«. Tako bodo vsebino videli samo tisti, ki jih imamo na svojem seznamu FB prijateljev. Nastavitev vidnosti objav samo prijateljem je diskreten ukrep za boljše varovanje zasebnosti. Tako uporabnik še naprej vzdržuje močne vezi s prijatelji, po drugi strani pa tovrstna izbira zmanjša potencial za vzpostavitev novih ali pojavljajočih se vezi, kar nekako naredi omrežje manj družbeno za uporabnike s takšnimi cilji (Stutzman in Kramer-Duffield 2010). Objave lahko omejimo tudi tako, da so vidne izključno nam. Zelo uporabna nastavitev je nastavitev po meri, kjer sami nastavimo, komu želimo omogočiti vidnost in komu ne. Poleg že prej omenjenih možnosti imamo tukaj še možnost delitve s prijatelji naših prijateljev, določenimi

ljudmi ali seznami, kjer sami navedemo imena ljudi, ki jim omogočamo ogled. Na sezname razvrščamo FB prijatelje v poljubne kategorije, kot denimo prijatelje iz šole, službe, različnih projektov in podobno. Seznami so z vidika zasebnosti praktični, saj lahko za vsak seznam posebej nastavimo drugačne nastavitve in tako onemogočimo, na primer vsem sodelavcem naenkrat vidnost objav ali fotografij, ki bi lahko negativno vplivale na našo kariero. Seznami so zelo koristni pri osebah z velikim številom prijateljev, saj imajo tako lažji pregled nad njimi, prav tako pa je lažje določiti nastavitve za cel seznam, kakor za vsakega posameznika. Leta 2011 se je pojavila možnost dodajanja ljudi na seznam znancev. Ta možnost omogoča uporabnikom, da lahko ljudi, s katerimi niso v rednem kontaktu ali enostavno ne želijo pogosto spremljati njihovih objav, preprosto dodajo na seznam znancev. Ciljno deljenje vsebine z različnim občinstvom, kot smo ga opisali tukaj, je ena izmed preventivnih strategij, ki pomagajo pri uravnavanju zasebnosti in javnosti s preprečevanjem neprijetnih situacij za sebe ali druge (Lampinen in drugi 2011).
Kljub prednostim, ki jih seznami prinašajo, pa so pretekle raziskave pokazale, da se malo uporabnikov poslužuje seznamov, saj naj bi jih ustvarilo in uporabljalo le 5 %. (Gummadi in drugi 2013).

Objave lahko delimo tudi s prijatelji označenih oseb. Nastavitve vidnosti objav so bile do nedavnega privzeto nastavljene kot javne, kar pomeni, da je objave lahko videl vsak uporabnik Facebooka. V maju 2014 pa so uvedli spremembo, ki novim uporabnikom nastavi vidnost objav privzeto na njihove Facebook prijatelje. Kot dodaten opomnik uporabniku, da se prepriča, s kom bo delil vsebino, je tudi funkcija »Privacy Checkup« (slika 5.3), ki se pojavi kot pojavno okno, preden želi nekaj objaviti na Facebooku (Facebook 2014).

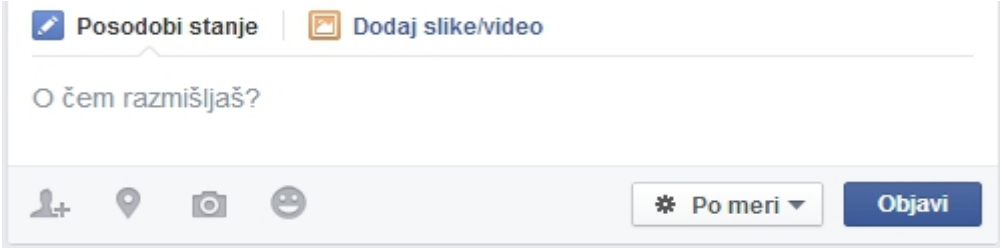
Slika 5. 3: Privacy Checkup



Vir: Facebook.com (2014).

Orodja za vidnost objav si zapomnijo občinstvo, ki smo ga nastavili ob zadnji objavi in tako samodejno uporabijo isto občinstvo ob ponovni objavi na zidu. Nastavitve lahko preprosto spremenimo kar pod oknom za posodobitev stanja, kjer imamo poleg gumba za objavo na voljo gumb z različnimi možnostmi občinstva (slika 5.4). Ta možnost je uporabniku na voljo tudi pod obstoječimi objavami na profilu, kjer lahko vidi, komu so namenjene, ima pa tudi možnost preteklim objavam spremeniti občinstvo.

Slika 5. 4: Nastavljanje občinstva pred objavo



Vir: Facebook.com (2014).

Dnevnik dejavnosti

V kategoriji vidnosti objav lahko pregledamo dnevnik dejavnosti, kaj smo do sedaj objavili, kaj komentirali, všečkali, koga sprejeli za prijatelja in podobno. Zraven tudi vidimo, katerim osebam je posamezna objava vidna. Dnevnik dejavnosti je razdeljen na več kategorij, saj lahko poleg vseh dejavnosti naenkrat, pregledamo po vsakem elementu posebej. Tako lahko posebej pogledamo časovnico, oznake, naše objave, objave drugih oseb, kjer smo označeni in objave, ki smo jih skrili in tako niso vidne na naši časovnici. Upravljamo lahko s fotografijami, ki smo jih naložili, na tistih, kjer smo označeni, pa lahko zgolj nastavimo, da ne želimo imeti vidne na svoji časovnici, kar pomeni, da bodo kljub temu še vedno vidne tistemu, ki jih je naložil in njegovim prijateljem. V dnevniku dejavnosti imamo pregled nad vsem, kar nam je bilo všeč, od strani in zanimanj do objav in komentarjev prijateljev. Pregledamo lahko pretekle komentarje, spremembe na našem profilu (sprememba prikazne fotografije, dodajanje interesov, službe ...), zgodovino prijateljstva. Med drugim lahko vidimo tudi seznam iskanj (oseb, dogodkov, strani in podobno), kar je samodejno nastavljeno, da je vidno samo nam. Dnevnik dejavnosti je zelo koristna stvar, ko želimo pregled nad vso vsebino, organizirano kronološko in po kategorijah.

Nastavljanje stikov

V tej kategoriji lahko nastavimo, kdo nam lahko pošlje prošnjo za Facebook prijateljstvo. Privzeto je to nastavljeno na »vsi«, kar pomeni, da lahko kdor koli zaprosi za naše prijateljstvo, mi pa se potem odločimo, ali bomo to osebo sprejeli ali ne. Nastavitev lahko spremenimo tudi tako, da nas lahko poiščejo le prijatelji naših prijateljev na Facebooku. V primeru da se za potrditev prijateljstva odločimo, bo oseba dobila potrditveno obvestilo, v nasprotnem primeru pa ne bo vedela, da smo jo zavrnili.

Nastavitev iskanja

Gre za možnost, da nas lahko nekdo poišče na Facebooku na različne načine. Uporabnik ima v tem sklopu na voljo tri kategorije iskanja. Prva kategorija se nanaša na iskanje preko navedenega elektronskega naslova, ki smo ga navedli ob pridružitvi k omrežju. Izbiramo lahko med prijatelji, prijatelji prijateljev in vsemi uporabniki. Naslednja kategorija je iskanje preko navedene telefonske številke in zadnja, ki omogoča, da se drugi iskalniki povežejo z našim profilom in ga tako pokažejo med rezultati iskanja. To pomeni, da ko nekdo v iskalnik vnese naše ime in priimek, mu bo Facebook kot rezultat vrnil povezavo do našega profila in ponudil možnost prijateljevanja. Z izklopom te možnosti zahtevamo, da se naš profil ne prikaže med rezultati iskanja, kar po eni strani pripomore k večji zasebnosti, po drugi strani pa prepreči

nekomu, da bi nas poiskal in dodal za prijatelja. Do sklenitve prijateljstva lahko pride, če mi dodamo to osebo ali nas predlaga nekdo od naših obstoječih Facebook prijateljev.

5.3. Nastavitve za časovnico in označevanje

V sklopu zasebnosti je tudi področje, kjer lahko nastavljamo vse v zvezi s časovnico in oznakami.

Slika 5. 5: Nastavitve za časovnico in označevanje

Vir: Facebook (2014).

Zgoraj (slika 5.5) je razvidno, da so nastavitve razdeljene na tri sklope s podkategorijami. Prvi sklop se nanaša na objave in oznake, ki se prikažejo na uporabnikovi časovnici. Lahko nastavimo ali dovolimo svojim prijateljem objavo stvari na naši časovnici ali pa bomo samo mi tisti, ki bomo lahko objavljali. Drugi sklop predstavlja nastavitve vidnosti objav in oznak na naši strani. Najprej lahko preverimo, kako drugi vidijo našo časovnico. Opcija omogoča, da vidimo, kako Facebook prikaže našo časovnico javnosti in kako jo vidi kdo od posameznih prijateljev. Ta funkcija je že nekaj časa dostopna tudi na uporabnikovi profilni strani, in sicer na desni strani naslovne fotografije, kar uporabniku olajša iskanje med drugimi nastavitvami. Nadalje lahko nastavimo vidnost objav, v katerih smo bili označeni, in vidnost prijateljevih objav na naši časovnici. Zadnji sklop teh nastavitev se nanaša na upravljanje z oznakami in predlogi zanje, ki jih dodajo drugi ljudje.

Označevanje ali »Tagging«

Označevanje smo že omenili pri nastavitvah vidnosti objav, ker pa se oznake vse pogosteje uporabljajo na družbenih omrežjih in se z njimi odpirajo tudi nekatera vprašanja zasebnosti, je smiselno temu področju nameniti nekaj besed. Označevanje je dodajanje hiperpovezave na profil označene osebe.

Običajno se nanaša na osebe, lahko pa tudi na oznako lokacije. Najpogosteje se srečujemo z oznakami oseb na fotografijah, kjer nekdo na fotografiji označi osebo in tako ustvari povezavo do te le-te. Označen uporabnik je ob tem obveščen in se, v primeru da ima omogočeno nastavitev pregleda objav, lahko odloči, ali želi odobriti objave, preden se pojavijo na njegovi časovnici. Lahko nastavi tudi, komu bodo vidne objave z našo oznako. Vendar se tukaj pojavi težava. Uporabnik sicer lahko vpliva na vidnost objav, ki se pojavijo na njegovem zidu. Toda v primeru, da nimamo nastavljenega pregleda oznak in nas označi naš prijatelj na svoji fotografiji, bo ta vseeno vidna na njegovem profilu njegovim prijateljem, ki niso nujno naši prijatelji. Težave lahko nastopijo, če gre za neprimerne fotografije ali stanja, kjer je uporabnik označen in ne ukrepa pravočasno. Takšne situacije so pogoste na družbenih omrežjih in se pojavijo kljub prizadevanjem za preprečevanje spodrsljajev. Po besedah raziskovalcev (Lampinen in drugi 2011) se takrat obrnemo h korektivnim strategijam, če začutimo potrebo po ponovni pridobitvi nadzora. Ena izmed tovrstnih strategij je brisanje oznak ali komentarjev. Če to ne uspe, lahko prosimo uporabnika, ki je vsebino naložil, da jo izbriše. V skrajni sili obstaja tudi prijava administratorjem na Facebooku, kjer navedemo razlog, zakaj želimo, da se nekaj odstrani, vendar mora za uresničitev cilja biti vloženih več prijav zoper isto zadevo. Omeniti je potrebno, da korektivne strategije niso vedno najboljša rešitev in se je bolje posluževati preventivnih strategij, ki smo jih omenili predhodno.

Predlagane oznake po prepoznavi obrazov

Pred časom se je Facebook povezal s tehnološkim podjetjem Face.com, ki je razvilo zelo napredno platformo za učinkovito prepoznavanje obrazov pri naloženih fotografijah. Pri Facebooku to pomeni avtomatizirano prepoznavanje obrazov ljudi s pomočjo programske opreme. Facebook je storitev uveljavil kot privzeto za vse uporabnike, namesto da bi omogočil, da uporabniki sami izberejo, ali želijo, da Facebook digitalno prepozna njihov obraz. Eden od ciljev te opcije je, da označevanje poteka hitreje in lažje. Program naj bi namreč sam po pregledu fotografij predlagal oznake uporabnikov, namesto da jih označujemo na vsaki fotografiji posebej. Večkrat ko je oseba označena na fotografijah, bolj natančna platforma za prepoznavanje obrazov postane.

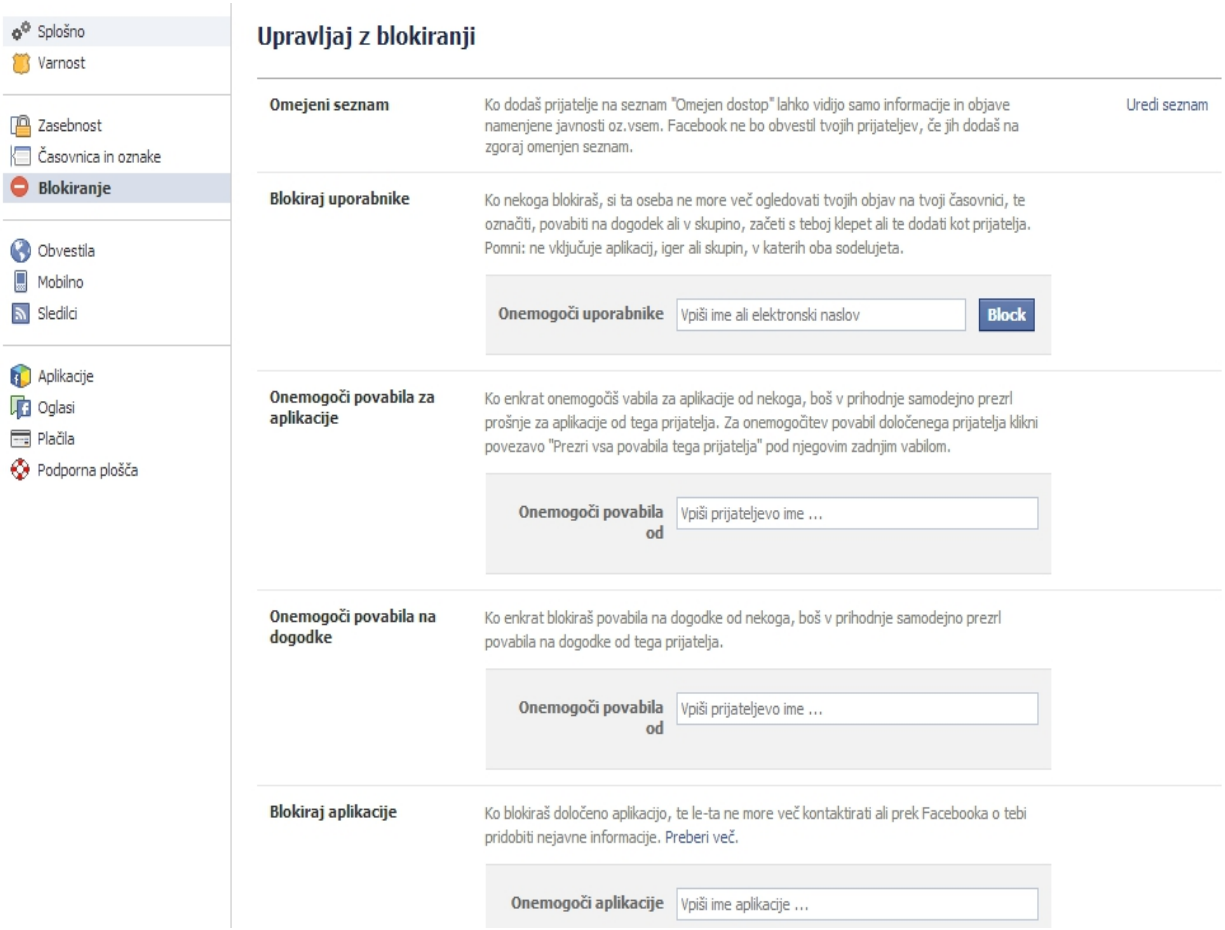
Storitev pri nas zaenkrat še ni na voljo, čeprav je možnost vključena v kategoriji upravljanja oznak. Nekod drugod po svetu storitev že deluje, so se pa že pojavili pomisleki, da s tem Facebook spodkopava spletno zasebnost svojih uporabnikov (Shaw 2012).

5.4. Blokiranje

Omenjena kategorija (slika 5.6) uporabniku omogoča, da lahko omeji ali celo onemogoči dostop nekaterim Facebook prijateljem. V kategoriji imamo več podkategorij za urejanje, in sicer:

- Omejeni seznam – Ta omogoča, da nastavimo prijateljem omejen dostop, kar pomeni, da bodo lahko videli le objave namenjene javnosti.
- Blokiraj uporabnike – Osebi, ki jo blokiramo, preprečimo ogled naših objav, povabila na dogodke ali skupine, označevanje, klepet in ji tudi onemogočimo prošnjo za prijateljstvo. Blokirana oseba lahko vseeno vidi naše objave, če smo predhodno člani iste skupine ali uporabljamo iste aplikacije.
- Onemogoči povabila za aplikacije – Aplikacije smo že omenili. Na Facebooku jih je vedno več, ki uporabnikom nudijo veliko zabave. Veliko od njih je takšnih, ki od uporabnikov v zameno za določene bonuse znotraj aplikacije zahtevajo, da povabijo še svoje prijatelje. Tako se pogosto zgodi, da prejemamo razna prijateljeva povabila k igranju takšne ali drugačne aplikacije (v večini primerov gre za igre). Ta možnost omogoča, da navedemo osebo, od katere ne želimo več prejemati prošenj za aplikacije. Vsa nadaljnja vabila od te osebe bodo prezrta.
- Onemogoči povabila na dogodke – Tukaj gre za zelo podobno zadevo, le da se nanaša na dogodke. Rešitev je enaka. Ko onemogočimo povabila od osebe, bodo vsa nadaljnja povabila prezrta.
- Blokiraj aplikacije – Možnost omogoča, da aplikacijo blokiramo, da ne more več pridobivati naših podatkov. Vseeno se lahko zgodi, če smo aplikaciji zaupali elektronski naslov, da nam bo ta vseeno pošiljala pošto nanj. Zadeva se reši tako, da v prejetem sporočilu kliknemo na povezavo za odjavo od prejemanja novic.

Slika 5. 6: Prikaz nastavitev v kategoriji blokiranje



Vir: Facebook (2014).

5.4 Ostale nastavitve

Znotraj nastavitev se nahajajo še druge kategorije, ki se posredno nanašajo na zasebnost. Te bomo zgolj na kratko predstavili, saj ne igrajo tako bistvene vloge, kakor tiste, ki smo jih prej že izpostavili.

5.4.1 Nastavitve obvestil

Pri tej nastavitvi gre predvsem za možnosti, kako in o čem želimo prejemati obvestila. Obvestila prejemamo normalno preko Facebooka, lahko pa nastavimo tudi prejemanje preko elektronske pošte ali preko mobilnega telefona, če ima naloženo Facebook aplikacijo.

5.4.2 Mobilne nastavitve

Aktivacija te možnosti omogoča pošiljanje obvestil, prošenj, posodobitev na naš mobilni telefon. Odgovarjanje na zasebna sporočila in komentarje je možno kar preko SMS sporočil. Pri izbiri te možnosti je potrebno biti previden, saj lahko hitro nehote razkrijemo svojo telefonsko številko.

5.4.3 Sledilci

Včasih se je možnost imenovala naročniki. Gre za to, da omogočimo prikaz naših objav na glavni strani z objavami. Prijatelji so že privzeto naši sledilci in obratno, lahko pa omogočimo sledenje ali sami sledimo tudi ostalim ljudem, s katerimi nismo prijatelji. Sledilci vidijo objave, ki so namenjene javnosti, tako da če ima nekdo zelo zaseben profil, mu je nesmiselno slediti. Možnosti sledenja so pogoste pri znanih osebnostih, saj je Facebook omejil maksimalno število prijateljev na 5000, medtem ko za število sledilcev ni omejitev. Funkcija pa je postala popularna tudi na splošno v zadnjem času, ko sta se združila Facebook in še eno izredno popularno omrežje Instagram, ki podobno kot Twitter temelji na sledilcih. Na Facebooku se pojavlja zelo veliko profilov znanih oseb in blagovnih znamk, ki jim uporabniki sledijo, ti pa običajno niso pravi oziroma gre za profile, ki so jih ustvarili oboževalci. Nekateri profili so preverjeni s strani Facebooka in imajo tako zraven svojega imena tudi modro kljukico, ki potrjuje verodostojnost profila.

5.4.4 Aplikacije

V kategoriji aplikacij imamo seznam vseh aplikacij, ki smo jih kdaj uporabljali. Tem aplikacijam lahko nastavljamo vidnost, se pravi ali bodo javno vidne na našem profilu ali bomo nastavili katero izmed drugih prej omenjenih možnosti. Za vsako aplikacijo tudi piše, katere podatke uporablja in ali ji dovolimo dostop do objav v zbirniku novic in objavljanje v našem imenu. Naslednji sklop teh nastavitev se nanaša na posredovanje naših podatkov drugim osebam, ki uporabljajo iste aplikacije. Če to možnost onemogočimo, nam je posledično tudi onemogočena uporaba aplikacij in iger. Zadnji dve nastavitvi sta takojšnja prilagoditev in nastavitev za stare različice Facebooka za mobilnike. Takojšnja prilagoditev zaenkrat še ni na voljo pri nas, gre pa tukaj za partnerstvo Facebooka z drugimi spletnimi stranmi, ki jim posreduje naše osebne podatke. Bistvo tega je, da se partnerska spletna stran ob uporabnikovem prvem obisku personalizira in mu takoj pokaže denimo izdelke, glasbo, igre, ki so mu všeč. Zadnja nastavitev za mobilnike omogoča nadziranje zasebnosti stvari, ki jih objavljamo preko starejših mobilnih aplikacij, ki nimajo sprotnega izbiranja občinstva (Facebook 2014).

5.4.5 Oglasi

V nastavitvah za oglase imamo dva sklopa, in sicer za strani tretjih oseb ter za oglase in prijatelje. V prvem sklopu je navedeno, da Facebook ne daje pravice tretjim osebam (oglasnim

mrežam ali aplikacijam) do uporabe naših informacij. Nadalje piše, da v kolikor bodo to v prihodnosti dovolili, bo imel uporabnik možnost izbire, komu želi te informacije prikazati. Sklop »Oglasi in prijatelji« se nanaša na povezovanje oglasov s prijatelji, kar naj bi pomagalo uporabnikom najti izdelke in storitve na podlagi tega, kar so delili in všečkali prijatelji. Tako je ob omogočanju te nastavitve pod oglasom prikazano tudi, da je uporabniku izdelek ali storitev, ki se ga oglašuje, všeč.

6 UGOTOVITVE

Po pregledu nastavitev, ki jih Facebook ponuja, ugotovimo, da je pri večini glavna naloga nastavljanje vidnosti uporabnikovih informacij in vsebine. Širok nabor možnosti uporabniku omogoča, da poskrbi za svojo zasebnost, v kolikšni meri pa je odvisno od njegovih interesov in tega, koliko se bo poglobil v posamezne nastavitve, da bi razumel njihovo delovanje. Nekaj nastavitev je resda malce nerazumljivih uporabniku – denimo zasledili smo dve podobni nastavitvi – prvo v sklopu Zasebnost, kjer se nahaja nastavitev »Kdo lahko vidi moje stvari?« in drugo v sklopu Časovnica in oznake, kjer imamo nastavitev »Kdo lahko vidi stvari na moji časovnici?« Prva nastavitev se nanaša na splošno na naše objave v prihodnosti in na omejitev preteklih objav. Znotraj te nastavitve je še dnevnik dejavnosti, kjer lahko pregledamo zgodovino vseh naših dejanj (objave, komentarji, všečki in oznake) in dejanj drugih, ki so povezana z nami (objave, komentarji in oznake na našem profilu).

Pri drugi nastavitvi imamo možnost pregleda, kako našo vsebino na časovnici vidi določen prijatelj. Naslednja možnost je nastavitev vidnosti objav, kjer smo bili označeni in nastavitev vidnosti prijateljevih objav na naši časovnici. Tukaj zasledimo podobnost s prej omenjenimi možnostmi vidnosti prihodnjih in preteklih objav. Razlika je v tem, da gre tukaj zgolj za dejanja FB-ovih prijateljev, torej njihove objave na našem profilu ter uporaba oznak, ki lahko nekoga preusmerijo do nas. Kot smo omenili, da bi razumeli neko posamezno nastavitev, jo je najprej potrebno dobro preučiti in preveriti kako deluje, drugače lahko komu nezavedno razkrijemo, kar nismo želeli.

Kot uporabniki pa z upravljanjem nekaterih nastavitev nimamo vedno popolne kontrole, saj se nekatere navezujejo na vsebino, ki si jo delimo s prijatelji. To so denimo oznake, kjer lahko nastavimo, da se vsebina, ki se navezuje na nas, ne bo prikazala na naši časovnici, težje pa je preprečiti, da se to prikaže na profilu tistega, ki nas je označil. Facebook temelji na povezavah med uporabniki in tako je na neki povezavi možno zagotoviti popolno zasebnost le, če imata oba uporabnika postavljene iste kriterije za vidnost podatkov. Podobno je pri seznamu prijateljev, kjer se med dvema osebama, ki skleneta prijateljstvo, to lahko prikaže na časovnici ali v zbirniku

novic. V kolikor omejimo vidnost tega, prijatelj pa ne stori enako, bodo skupni prijatelji to novico vseeno videli pri njemu.

Kot smo že omenili, tudi Facebook zbira naše podatke, prijavne in tiste, za katere smo sami določili deliti na SSO. Zbira pa tudi druge podatke, metapodatke, ki jih pridobi na podlagi naših objav in sprememb. Če vzamemo za primer Facebook klepet, je ta narejen tako, da razkrije več, kot bi želeli. Denimo, ko uporabnik prebere prejeto sporočilo, se to pošiljatelju prikaže kot prebrano. Kadar komuniciramo z nekom preko mobilnega telefona, se ob poslanem sporočilu zraven izpiše še lokacija, od koder smo ga v tistem trenutku poslali. Tukaj gre seveda za poseg v zasebnost uporabnika, nastavitve za onemogočanje teh funkcij pa Facebook nima. Zadeva se da sicer rešiti z različnimi razširitvenimi vtičniki, ki pa jih je treba prenesti od drugod.

Opaziti je, da Facebook z vsako večjo spremembo, bodisi vizualnega izgleda omrežja (časovnica) ali z dodajanjem različnih novih in privlačnih aplikacij, nekoliko spremeni tudi upravljanje zasebnosti, da se lahko prilagodi posodobitvam. Uporabniki morajo tako spoznati novosti, se na njih navaditi, med drugim pa tudi ponovno preučiti, kako upravljati z zasebnostjo, da ne bo prišlo do neželenega razkritja osebnih podatkov. Posebno pozorni morajo biti pri uporabi aplikacij, ki so običajno produkt zunanjih razvijalcev, ki niso del Facebooka. Aplikacije lahko zahtevajo veliko osebnih podatkov, zato je potrebno dobro prebrati, katere podatke potrebuje aplikacija za delovanje in kako jih bo uporabila.

7 SKLEP IN ZAKLJUČEK

Skozi diplomsko delo smo spoznali, kaj pravzaprav pomeni koncept upravljanja zasebnosti in kako se odraža pri spletnem družbenem omrežju Facebook. Upravljanje zasebnosti je tako v veliki meri odvisno od vsakega posameznika, k temu pa posledično, v konkretnem primeru Facebooka, pripomorejo tudi različne nastavitve zasebnosti. Spoznali smo glavne nastavitve povezane z zasebnostjo, kaj lahko z njimi spreminjamo in kako pripomoremo k večji zasebnosti. Omenili smo nekaj ključnih lastnosti in sprememb družbenega omrežja z vidika zasebnosti, kot so denimo aplikacije, oglaševanje ter časovnica – vizualna in tehnična sprememba postavitve Facebook profilov. Pregledali in preučili smo tudi ostale nastavitve, ki so posredno povezane z zasebnostjo in jih na kratko predstavili.

Zavedati se moramo, da se zasebnost na spletu obravnava in dojema drugače kakor v realnosti, pri neposrednem komuniciranju. Pri Facebooku je potrebno dobro razumeti politiko zasebnosti in delovanje posameznih nastavitev. Toda kljub temu uporaba teh nastavitev včasih ne zagotavlja popolne zasebnosti, saj na to vpliva več dejavnikov.

V prvi vrsti mora biti uporabnik previden pri tem, kaj deli in s kom ter katerih aplikacij se bo posluževal. Ustvariti si mora določene meje, saj mu lahko navidezne koristi ob uporabi različnih storitev namesto pričakovanih prednosti povzročijo škodo, v smislu zlorabe osebnih informacij, ogrozitve kariere, kraje identitete in še česa drugega. Kot uporabniki Facebooka smo večkrat postavljeni pred dilemo, ali objavimo nekaj in delimo z drugimi ali je morda bolje, da nekatere stvari le zadržimo zase. Splet je namreč javni prostor, kjer lahko vsak dostopa do podatkov in z malce znanja je v iskalnikih možno poiskati naše starejše fotografije in se tudi dokopati do objav, ki smo jih morda nekoč brezskrbno objavljali na svoje profile družbenih omrežij. Drugi dejavnik, na katerega sami nimamo bistvenega vpliva, je nadzor vsebine, ki jo lahko drugi razkrijejo o nas, bodisi z objavami bodisi z oznakami na fotografijah.

Če želimo imeti več zasebnosti, se je koristno odstraniti iz rezultatov spletnih iskalnikov, ki ob vnosu našega imena in priimka ne bodo dali rezultatov in povezave do našega Facebook profila.

Podobno lahko naredimo tudi za iskanje znotraj Facebooka, kjer lahko nastavimo, da nas poiščejo zgolj prijatelji, kar nas bo popolnoma umaknilo iz rezultata iskanj na Facebooku. V kolikor tega ne želimo, pa lahko nastavimo, da nas lahko poiščejo tudi prijatelji naših prijateljev (Informacijski pooblaščenec RS 2010*)*.

Moja zaključna misel je ta, da je kljub vsem polemikam glede vprašanj zasebnosti na Facebooku ter ostalih družbenih omrežij, le-ta možno varno uporabljati, če se seznanimo s politiko zasebnosti posameznega omrežja, se naučimo čemu služijo določene nastavitve in spremljamo morebitne spremembe. Seveda pa Facebook ne zagotavlja popolne zasebnosti, saj gre za spletno socialno omrežje, ki je namenjeno povezovanju, druženju in je posledično za uresničitev tega potrebno razkriti določen minimum osebnih informacij. Pomembno je, da v prvi vrsti sami pri sebi določimo, kako bomo uporabljali Facebook, kako upravljali z zasebnostjo in do kolikšne mere bodo naši spletni profili odprti oziroma zaprti.

8 LITERATURA

1. Acquisti, Alessandro in Ralph Gross. 2006. *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*. Dostopno prek: http://people.cs.pitt.edu/~chang/265/proj10/zim/imaginedcom.pdf (7. maj 2014).
2. Al-Shakhouri, N.S. in Mahmood, A. »*Privacy in the digital world: Towards international legislation*«. Dostopno prek: http://firstmonday.org/ojs/index.php/fm/article/view/2146/2153 (6. maj 2014).
3. Blank, Grant, Gillian Bolsover in Elizabeth Dubois. 2014. *A New Privacy Paradox: Young people and privacy on social network sites*. Dostopno prek:http://www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%20April%202014.pdf (13.september 2014).
4. Boyd, Danah M. in Nicole B. Ellison. 2007. *Social Network Sites: Definiton, History, and Scholarship*. Dostopno prek: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full (30. december 2013).
5. Boyd, Danah in Eszter Hargittai. 2010. *Facebook privacy settings: Who cares?*. Dostopno prek: http://firstmonday.org/article/view/3086/2589 (30. december 2013).
6. Boyd, Danah in Alice Marvick. 2011. *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*. Dostopno prek: http://www.danah.org/papers/2011/SocialPrivacyPLSC-Draft.pdf (12. marec 2014).

7. Butler, Elizabeth, Elizabeth McCann in Joseph Thomas. 2011. *Privacy Setting Awareness on Facebook and its Effect on User-Posted Content*. Dostopno prek: http://www.uab.edu/Communicationstudies/humancommunication/04_01_2011_Butler (6. februar 2014).
8. Catlett, Jenna. 2007. *An Analysis of Female University Students' Communicative Management of Privacy Online via Facebook*. Dostopno prek: http://citation.allacademic.com//meta/p_mla_apa_research_citation/1/9/3/3/6/pages193365/p193365-4.php (12. maj 2014).
9. Cavusoglu, Husein, Tuan Phan in Hasan Cavusoglu. 2013. *Do Privacy Controls Influence Content Generation and Sharing Patterns of Online Social Network Users? A Natural Experiment*. Dostopno prek: http://weis2013.econinfosec.org/papers/CavusogluWEIS2013.pdf (4. januar 2014).
10. Chung, Winnie in John Paynter. 2002. *Privacy Issues on the Internet*. Dostopno prek: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.4421&rep=rep1&type=pdf (6. maj 2014).
11. Cutillo, Leucio Antonio in Refik Molva. 2009. *Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust*. Dostopno prek: http://www.p2p.tu-darmstadt.de/fileadmin/user_upload/Group_P2P/share/p2p-ws10/safebook.pdf (4. februar 2014).
12. Das, Indrama. 2014. *Studies of Privacy Issues in Online Social Networks*. Dostopno prek:

https://dspace.jdvu.ac.in/bitstream/123456789/29123/1/Acc.%20No.%20DC%201554.pdf (13. september 2014).

13. Day,S. 2013. *Self-disclosure on Facebook: How much do we really reveal?*. Dostopno prek: http://www.citrenz.ac.nz/jacit/JACIT1701/2013Day_Facebook.html (8. junij 2014).
14. Debatin, Bernhard, Jeannette P. Lovejoy, Ann-Kathtrin Horn M.A. in Brittany N. Hughes. 2009. *Facebook and Online Privacy: Attitudes, Behaviours, and Unintended Consequences*. Dostopno prek: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2009.01494.x/full (4. februar 2014).
15. Dourish, Paul in Leysia Palen. 2003. *Unpacking »Privacy« for a Networked World*. Dostopno prek: http://www.cs.cmu.edu/~jasonh/courses/ubicomp-sp2007/papers/06-palen-dourish.pdf (7. januar 2014)
16. Duggan, Maeve in Aaron Smith. 2013. *Social Media Update 2013*. Dostopno prek: http://www.pewinternet.org/2013/12/30/social-media-update-2013/ (10. maj 2014).
17. Dwyer, Catherine. 2008. *Appropriation of Privacy Management Within Social Networking Sites*. Dostopno prek: http://archives.njit.edu/vol01/etd/2000s/2008/njit-etd2008-058/njit-etd2008-058.pdf (16.september 2014).
18. Dwyer, Catherine, Starr Roxanne Hiltz, Marshall Scott Poole, Julia Gußner, Felicitas Hennig, Sebastian Osswald, Sandra Schilieẞlberger in Birgit Warth. 2010. *Developing Reliable Measures of Privacy Management Within Social Networking Sites*. Dostopno prek: http://www.computer.org/csdl/proceedings/hicss/2010/3869/00/07-08-03.pdf (10. maj 2014).

19. Egele, Manuel, Andreas Moser, Christopher Kruegel in Engin Kirda. 2012. *PoX: Protecting Users from Malicious Facebook Applications*. Dostopno prek: http://seclab.tuwien.ac.at/papers/pox-journal.pdf (10. februar 2014).
20. Ellison, Nicole B. In Dannah Boyd. 2013. Chapter 8: *Sociality through Social Network Sites*. Dostopno prek: http://www.danah.org/papers/2013/SocialityThruSNS-preprint.pdf (9. maj 2014).
21. Facebook. Dostopno prek: https://www.facebook.com/ (30. december 2013).
22. ---. Dostopno prek: https://www.facebook.com/facebook/info (11.september 2014).
23. ---. Dostopno prek: https://developers.facebook.com/docs/graph-api (14.september 2014).
24. ---. *Statement of Rights and Responsibilities*. Dostopno prek: https://www.facebook.com/legal/terms (18.september 2014).
25. Gabor, Milan. 2013. *Digitalni jaz in naše digitalne sledi*. Dostopno prek: http://www.viris.si/wp-content/uploads/2013/09/Digitalni-jaz-in-nase-sledi-20121.pdf (8. maj 2014).
26. Gjoka, Minas,Michael Sirivianos, Athina Markopoulou in Xiaowei Yang. 2008. *Poking Facebook: Characterization of OSN Applications*. Dostopno prek: https://www.cs.duke.edu/~xwy/publications/poking-facebook.pdf (5. februar 2014).
27. Govani, Tabreez in Harriet Pashley. 2005. *Student Awareness of the Privacy Implications When Using Facebook*. Dostopno prek: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf (10. maj 2014).

28. Gross, Ralph in Alessandro Acquisti. 2005. *Information Revelation and Privacy in Online Social Networks*. Dostopno prek: https://people.cs.pitt.edu/~chang/265/proj10/zim/inforevelation.pdf (12. maj 2014).
29. Gummadi, Krishna, B, Krishnamurthy in A. Mislove. 2013. *Addressing the privacy management crisis in online social networks*. Dostopno prek: https://www.iab.org/wp-content/IAB-uploads/2012/01/alan_mislove.pdf (7. junij 2014).
30. Ho, Thanh Ai. 2012. *Towards a Privacy-enhanced Social Networking Site*. Dostopno prek: https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/8581/Ho_Ai_2012_these.pdf;jsessionid=FF00E6D252E87B37023D35C81841622D?sequence=4 (8.september 2014).
31. Informacijski Pooblaščenec Republike Slovenije. 2010. *10 nastavitev zasebnosti, ki bi jih moral poznati vsak uporabnik Facebooka*. Dostopno prek: https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Kako_uporabljati_FB_in_preziveti_tisk__v2_-net.pdf (20. marec 2014).
32. Kayne, R. In O. Wallace. 2014. *What are Third Party Applications?*. Dostopno prek: http://www.wisegeek.org/what-are-third-party-applications.htm (17. maj 2014).
33. Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana. Mirovni inštitut.
34. ---. 2006. *Nadzor in zasebnost v informacijski družbi*. Ljubljana. Znanstvena knjižnica FDV.
35. Lampinen, Airi, Vilma Lehtinen, Asko Lehmuskallio in Sakari Tamminen. 2011. *We're in It Together: Interpersonal Management of Disclosure in Social Network Services*.

Dostopno prek:

https://www.academia.edu/1296538/Were_in_it_together_interpersonal_management_of_disclosure_in_social_network_services (6. februar 2014).

36. Lee, Ki Jung. 2013. *Development and Analyses of Privacy Management Models in Online Social Networks based on Communication Privacy Management Theory*. Dostopno prek:

http://dspace.library.drexel.edu/bitstream/1860/4108/1/Lee_KijungPhD.pdf (10. maj 2014).

37. Madden, Mary, Susannah Fox, Aaron Smith in Jessica Vitak. 2007. *Digital Footprints. Online identity management and search in the age of transparency*. Dostopno prek:

http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf (8. maj 2014).

38. Madejski, Michelle, Maritza Lupe Johnson in Steven Michael Bellovin. 2011. *The Failure of Online Social Network Privacy Settings*. Dostopno prek:

http://academiccommons.columbia.edu/catalog/ac:135406 (4. februar 2014).

39. ---. 2012. *A Study of Privacy Settings Errors in an Online Social Network*. Dostopno prek: http://www1.cs.columbia.edu/~maritzaj/publications/2012-sesoc.pdf (21. September 2014).

40. Minkus, Tehila in Memon N. 2014. *On a Scale from 1 to 10, How Private Are You? Scoring Facebook Privacy Settings*. Dostopno prek:

http://cse.poly.edu/~tehila/pubs/Usec2014.pdf (8. junij 2014).

41. Mislove, Alan, Massimiliano Marcon, Krishna P. Gummadi, Peter Druschel in Bobby Bhattacharjee. 2007. *Measurement and Analysis of Online Social Networks*. Dostopno prek: http://conferences.sigcomm.org/imc/2007/papers/imc170.pdf (10. maj 2014).
42. Mondal, Mainack, Peter Druschel, Krishna P. Gummadi in Alan Mislove. 2014. *Beyond Access Control: Managing Online Privacy via Exposure*. Dostopno prek: http://www.mpi-sws.org/~mainack/papers/usec2014-final46.pdf (19.september 2014).
43. Mohamed, Azza Abdel-Azim. 2010. *Online Privacy Concerns Among Social Networks' Users*. Dostopno prek: http://cscanada.net/index.php/ccc/article/viewFile/1003/1022 (4. januar 2014).
44. Netchitailova, Ekaterina. 2012. *Facebook as a Surveillance Tool: From the Perspective of the User*. Dostopno prek: http://www.triple-c.at/index.php/tripleC/article/view/404/408 (16. april 2014).
45. O'Brien, Deirdre in Ann M. Torres. 2012. *Social Networking and Online Privacy: Facebook Users' Perceptions*. Dostopno prek: http://aran.library.nuigalway.ie/xmlui/handle/10379/4059 (8. junij 2014).
46. Pearson, Siani in Marco Casassa Mont. 2011. *Sticky Policies: An Approach for Managing Privacy Across Multiple Parties*. Dostopno prek: https://documents.epfl.ch/users/a/ay/ayday/www/mini_project/Sticky%20Policies.pdf (15.september 2014).
47. Petronio, Sandra in Irwin Altman. 2002. *Boundaries of Privacy*. Dostopno prek: http://muse.jhu.edu/books/9780791487853?auth=0 (20. marec 2014)

48. Rui, Jian in Michael A. Stefanone. 2012. *Strategic self-presentation online: A cross-cultural study*. Dostopno prek: http://www.sciencedirect.com/science/article/pii/S0747563212002257 (23.september 2014).
49. Shaw, Lisa. 2012. *Facebook's Facial Recognition Technology*. Dostopno prek: http://parentingtodayskids.com/article/danger-facebooks-facial-recognition-technology/ (13. februar 2014).
50. SI-CERT. *Parazitni programi; Adware, Spyware in prikrita omrežja*. 2002. Dostopno prek: https://www.cert.si/si-cert-2002-ciactech02-004-parazitni-programi/ (14.september 2014).
51. Socialbakers. Dostopno prek: http://www.socialbakers.com/facebook-statistics/slovenia (5. februar 2014).
52. Stal, Mihkail in Martin S. Fiebert. 2013. *Changes in Facebook Behaviour Over Time*. Dostopno prek: http://computerresearch.org/stpr/index.php/gjcst/article/download/1445/1311 (16. maj 2014).
53. Statistic Brain. Dostopno prek: http://www.statisticbrain.com/facebook-statistics/ (16. maj 2014).
54. Strater, Katherine in Heather Richter Lipford. 2008. *Strategies and Struggles with Privacy in an Online Social Networking Community*. Dostopno prek: http://hci.uncc.edu/wordpress/wp-content/uploads/2011/05/strategies-and-struggles.pdf (9. januar 2014).

55. Stutzman, Fred in Jacob Kramer-Duffield. 2010. *Friends Only: Examining a Privacy-Enhancing Behaviour in Facebook*. Dostopno prek: http://fredstutzman.com/papers/CHI2010_Stutzman.pdf (11. februar 2014).
56. The Graph API. Dostopno prek: https://developers.facebook.com/docs/graph-api (9. junij 2014).
57. Waters, Susan in James Ackerman. 2011. *Exploring Privacy Management on Facebook: Motivations and Percieved Consequences of Voluntary Disclosure*. Dostopno prek: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2011.01559.x/full (11. marec 2014).
58. Web Applications: *What are They? What of Them?*. 2014. Dostopno prek: http://www.acunetix.com/websitesecurity/web-applications/ (17. maj 2014).
59. Zimmerman, Rachel K. 1998. *The way the »cookies« crumble: Internet privacy and data protection in the twenty-first century*. Dostopno prek: http://www.merchantgould.com/resources/images/1310.pdf (8. maj 2014).
60. Wisniewski, Pamela, Bart P. Knijnenburg in Heather Richter Lipford. 2014. *Profiling Facebook Users' Privacy Behaviours*. Dostopno prek: http://www.usabart.nl/portfolio/Wisniewskietal-pps2014.pdf (15.september 2014).