UDK:340.64(497.11)
Biblid 1451-3188, 10 (2011)
Год X, бр. 37–38, стр. 271–281
Изворни научни рад

Мр Сергеј УЉАНОВ[1]
Мр Звонимир ИВАНОВИЋ[2]

КРАЂА ИДЕНТИТЕТА У СРБИЈИ, РАСТУЋИ ПРОБЛЕМ

ABSTRACT

All existing applications on social network sites are intended to facilitate means of communication and as it is the case with some form of social prosthetics this raises a lot of questions. At this moment, the protection of privacy and personal data and their distribution is the question that is crucial for Serbia (and the world) since no adequate protection has been established in that field, this concerning everyone who publishes this kind of information online. For that kind of problem, we should just consider the sites of Serbian companies, which fail to protect their information and by that, they facilitate perpetrators in many ways in obtaining very personal and other valuable data from the Internet pages offering information on their employees. If we add to what has been previously said some alternative ways of obtaining information, we can just imagine the dimensions of possible exploiting and types of abuse. It is not hard to hypothesize, given the security measures that administrators of Facebook (or other networks or web 2.0 applications) carry out, that it can be easily exploited in various ways. It is very important to explore the current Serbian legislation dealing with the protection of Internet users, with special emphasis on social networking online, this also including other virtual spaces, which could provide various personal and other data. Every kind of information published on the Internet is irreversibly and permanently archived in the database of Internet Crawlers and in that way, it is accessible to anyone, what creates additional risk to the information owner (or someone close to him).

Key words: Social networks, Web 2.0 applications, legal protection of Internet users, identity theft, mobile social networks.

[1] МУП РС УКП, НЦБ ИНТЕРПОЛ Београд.

[2] КПА, Београд.

I) УВОДНА РАЗМАТРАЊА

У савременим оквирима информационог друштва појединац је незнатна јединка која чини глобално село, нарочито посматрано кроз призму савремених социјалних мрежа, као на пример *facebook*, *flicker* или *digg*, или друге мреже или *web* 2.0 апликације.[3] У погледу размера проблематике можемо само указати на постојеће податке о једној од поменутих мрежа. Историјат развоја Facebook-а према бројности корисника:[4]

Месец и година	Број активних корисника
Децембар 2004.	1.000.000
Децембар 2005.	5.500.000
Децембар 2006.	12.000.000
Октобар 2007.	50.000.000
Август 2008.	100.000.000
Јануар 2009.	150.000.000
Април 2009.	200.000.000
Јул 2009.	250.000.000
Септембар 2009.	300.000.000
Август 2010	Преко 500.000.000

Све постојеће апликације на социјалним мрежама замишљене су као облик средстава за олакшавање комуникације и као социјалне протезе, чиме се отварају многа питања. Питање приватности и заштите дистрибуције личних података је у овом тренутку у Србији (али и у свету) веома проблематично, не постоји адекватна заштита која се може пружити било коме у овом моменту ко је спреман, али можда можемо рећи и лаковеран, да своје личне податке и пратеће информације објави на

[3] Први пут овај термин је 1999. год. искористила Дарси Динући (Darcy DiNucci) у свом чланку „Фрагментарна будућност“ (Fragmented Future), а касније ју је О'Рајли група (O'Reilly Media) популарисала. Више о овоме на www.wikipedia.org\web2.0 доступној 23.01.2010.год.

[4] Интернет: http://www.facebook.com/press/info.php?timeline, доступно 02.02.2011. Један од значајних показатеља активности на Интернету је и да се више од 50% корисника логује свакодневно на ФБ, а најфрапантнији је податак да постоји више од 250.000.000 корисника који ФБ приступају путем мобилних телефонских уређаја.

Интернету.[5] За тако нешто није неопходна социјална мрежа, посматрајмо само фирме у Србији и њихове сајтове, код којих постоји прегршт путева да се прибаве многе, веома приватне и вредне, информације само са страница којима се описују запослени у њима.[6] Уколико овоме додамо још и могућности других облика прибављања информација, као на пример, један од облика који се веома дуго користи на западу – претурање по туђем ђубрету, или на пример, социјални инжењеринг, можемо само замислити димензије могућих злоупотреба.[7]

II) ПРЕДМЕТ РАДА

Свако од нас добија најразличитије рачуне на којима постоје наши лични подаци, чак и они којих нисмо сами свесни (типа: бројеви уговора у преплатничком односу са мобилним телефонијама, као и социјални контакти које имамо са различитим пријатељима – кроз листинге у тим рачунима и многи други). Колико се на ово може надовезати истраживање Sophos групе у којем је једна група истраживача у намери да прикаже недостатке социјалних мрежа креирала фиктивни лик гумене паткице у једном или гумене жабице, у другом истраживању, и пријавила се као пријатељ на социјалној мрежи одређеној групи људи.[8] Социјалне мреже

[5] Са овим се може поредити и глупост једног од предузетника из САД који је на свом аутобусу носио свој ССН (Social security number, број социјалногог осигурања, који је основно средство идентификације у САД). Наравно он је био жртва крађе идентитета.

[6] Довољно је видети странице које у име своје фирме а у вези својих запослених на Интернету постављају најразличитији послодавци без адекватних упутстава за запослене и без обавештавања о могућим ризицима.

[7] Којим се на најперфиднije начине извлаче информације најразличитијих нивоа тајности и значаја од људи.

[8] Овај истраживачки подухват двојице ентузијаста Софоса представља наставак или се чак може рећи продужетак претходног пројекта у Великој Британији (у питању је само огранак исте фирме софоса само у ВБ) када је главну улогу одиграла гумена жабица. Наиме такозвани пројекат Фејсбук сонде обухвата креирање фиктивног лика неке умиљате дечије играчке која је потпуно безазлена (у том случају гумене зелене жабице Freddie Staur 1980), како не би изазвала сумњу корисника и понудити пријатељство на социјалној мрежи са истом што је врло умиљато али открива недостатке овакве активности. Овај продужетак је обухватио креиррање фиктивних женских ликова (два Dinette Stonily педесет и нешто година старости а која је добила лик мачке која се игра и Daisy Feletin рођену 1988.год. са ликом гумене паткице) и ограничио се територијално на Аустралију, који су се појавили на нету и тражили пријатељство од по сто људи из њихове старосне групе. Након првих реакција

препуне су најразличитијих личних података постованих на профилима. Овај податак уопште није занемарив, управо у овом тренутку један колега из Турске спроводи анкету на Интернету о информацијама које имају личну конотацију, и које представљају основе права на приватност, као и расположивости истих на социјалним мрежама (он се определио за фејсбук).[9] Наравно ова активност је повезана са „дељењем" адекватне количине информација са прихваћеним контактима – пријатељима у социјалним мрежама, што даје посебну димензију овом пробоју информација. Ово се врши кроз подешавање опција приватности. Није тешко претпоставити, обзиром на безбедносне мере које администратори фејсбука (или других мрежа или web 2.0 апликација), да се исте могу јако лако злоупотребити на различите начине.[10] Довољно је проверити ниво заштите приватности неке од ових социјалних мрежа у тзв. изјавама о приватности.[11] У оквирима разматрања кроз призму Интернет технологија неки аутори дефинишу поверење као „воља и жеља одређене

постигао се исти резултат као у случају жабице 87 лица је прихватило пријатељство, али овог пута се отишло и даље петоро додатних људи се пријавило ниоткуда желећи пријатељство са једном од поменутих. Веома су интересантни резултати размене података „пријатеља" након постајања пријатељем па тако у групи од 20 година и нешто старости сви (100%) су разменили или учинили доступним персоналне адресе електронске поште док су у старијој групи њих 87% учинили исто. Са друге стране телефонски број је одало 23% старијих и 7% млађих, млађи су податке о својим члановима породице и пријатељима одали у 46% а старији у 31% и 89% млађих пун датум рођења а 57% старијих. Интернет: http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/

[9] За онога кога више интересује о овоме, анкету и појединостављења уз контакт може пронаћи на сајту: http://facebook-uses.questionpro.com/ доступном 18.01.2010. год.

[10] Интернет: http://www.facebook.com/terms.php?ref=pf доступан 20.01.2011. године, а последњи пут правила су ревидирана у октобру 2010. год., а такође и у вези са овим је политика приватности доступна истог датума на http://www.facebook.com/policy.php

[11] Довољно је само покушати да цитирамо један сегмент ове изјаве (неки је називају политика приватности) а фејсбук администратори сматрају да се њоме формирају принципи фејсбука: „предмет заштите права на приватност неће обухватати у социјалној мрежи (дакле представља јавну информацију доступну свима) податке који су постављени од стране корисника (дефинишући је сопственом одговорношћу поставиоца информације) и не може и неће се пружити заштита подацима и они могу бити предмет претраге на претраживачима, анализе других и трећих лица и сл". То значи да се претраживачима ипак у последњим изменама безбедносних критеријума ограничава могућност укључивања претрага приватно заштићених података, али остаје горући проблем лица која немају посебно адекватно знање енглеског језика и не могу да у потпуности испрате услове о којима се овде говори.

стране да постане рањива на активности друге стране засновано на очекивању да ће та друга страна предузети одређену активност значајну за лице које је носилац поверења, без обзира на могућност надзора или контроле те друге стране".[12] Поверење је критична детерминанта за трансфер или проток информација лицем у лице. Поверење је, такође, неопходна компонента за остваривање онлајн социјалних интеракција.[13] Нека истраживања указују на то да је поверење веома значајна компонента за размену информација у оквирима електронске трговине.[14] Студије случајева интерперсоналне размене потврђују да је поверење предуслов самоотварања, јер оно смањује ризик који садржи откривање личних информација.[15] Треба поменути да је приватност у социјалним мрежама често неочекивана или није дефинисана, социјалне мреже снимају све интеракције задржавајући их у циљу потенцијалне употребе при социјалном прикупљању података "data mining-u".[16] Реалне социјалне везе не остављају неки физички траг у спољашњој средини док се код дигиталног окружења оне јављају на сваком кораку.

III) АКТУЕЛНИ ВИДОВИ ПРОБЛЕМА

Све описано је нарочито значајно размотрити у оквирима актуелног стања у Србији у погледу правне регулативе у заштити корисника Интернета уопште, а посебно у оквирима социјалних мрежа, али и других виртуелних простора који могу открити најразличитије личне и друге податке и информације. Невероватна је количина неопрезности која се овом приликом манифестује, од стране најразличитијих профила корисника. Посебан аспект ове проблематике везује се за дечију психологију и дечје деловање у виртуелном свету, нарочито кроз неспособност деце да схвате значај прослеђивања различитих информација, различитим путевима на Интернету (где тата ради, како се његов тата зове, колико година има, када

[12] Mayer, R. C., J. H. Davis, and F. D. Schoorman (1995) "An Integrative Model of Organizational Trust," The *Academy of Management Review* (20) 3, pp. 709-734 (p. 712)

[13] Coppola, N., S. R. Hiltz, and N. Rotter (2004) "Building Trust in Virtual Teams," *IEEE Transactions on Professional Communication* (47) 2, pp. 95-104.

[14] Metzger, M. J. (2004) "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce 9 (4)," *Journal of Computer-Mediated Communication* (9) 4.

[15] Ibid.

[16] Dwyer, C. (2007) "Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study.

је рођен... и сл.).[17] Свака информација остављена на Интернету се неповратно архивира на неком од краулера, те је у сваком тренутку доступна а што је додатна опасност за онога ко ју је тамо оставио (или можда неког њему блиског). Веома је интересантно описано размотрити нарочито у светлу Есее агенде и Есее агенде плус и стратешком концепту развоја електронске управе у Србији постојање недостатака у планирању многих заштитних механизама у овом простору. Наиме све описано може имати значајне импликације на заштиту података о личности, и не само као у примеру колега из Аустралије да ће бити релативно лако могуће да се извади електронским путем возачка дозвола на лице рођено 1788. године, већ се могу веома брзо и лако створити нови употребљиви идентитети, који се могу продавати и користити у најразличитијим случајевима и на најразличитије начине.[18] Није од малог значаја чињеница да су Анто Готовина и Милорад Улемек – Легија имали хрватске пасоше из исте серије, што говори о сарадњи организованог криминала на нашим просторима не познајући националне границе и, до скора, чак зараћене стране.[19] Но, веома је проблематично на који начин се у Србији везује идентитет лица према

[17] Овај термин је добро одмерен јер треба имати у виду да администратори социјалних мрежа на пример фејсбука дозвољавају коришћење ове социјалне мреже само лицима старијим од 13 година, а што према категоризацијама у свету и даље обухвата популацију деце (код нас је до 14 година), а такође и друге категорије малолетних лица (млађи 14-16 и старији 16-18 година). Наравно, о њиховим способностима схватања значаја сопствених аката говори и Кривични законик и Закон о малолетним учиниоцима кривичних дела и кривично правној заштити малолетних лица, али и многе теоријске расправе.

[18] Персонално идентификујућа информација (енгл. Personally Identifiable Information, у даљем тексту PII), према ОМБ Меморандуму 07-16,12 (ОМБ), јесте "информација која се може користити да би се разликовао или пратио идентитет појединца, као што је његово име, SSN (енгл. Social Security Number), биометријски подаци и друге чињенице, појединачно или комбиновано са другим личним или идентификујућим информацијама које су повезане са одређеним појединцем, као што судатум и место рођења, девојачко презиме мајке и други подаци." Неки примери PII који идентификују појединца јесу (НИСТ, 2009): Име (име и презиме, надимак, девојачко презиме), лични идентификациони број (нпр. SSN, број пасоша, број текућег рачуна и друго), адреса (улица или e-mail адреса), број телефона, личне карактеристике (као што су фотографија лица или друге карактеристике, отисци прстију или друге биометријске слике). Такође у PII се убрајају и информације које су повезане са неком од следећих: датумом рођења, местом рођења, расом, религијом, запослењем, медицинске, едукативне или финансијске информације и друге. Видети интернет: http://www.youtube.com/watch?v=wrnYRPRF36E&feature=player_embedded# доступан 19.01.2011. год.

[19] Интернет: http://www.revija92.rs/code/navigate.php?Id=599&editionId=50&articleId=217 доступан 19.01.2010. год.

јавним службама, наиме рецимо претраге се у Јединственом информационом систему МУП-а раде најчешће и најтемељније преко ЈМБГ (Јединственог матичног броја грађана). Исти се генерише према унапред утврђеним правилима првих седам цифара означавају датум рођења, (дан, месец, годину без прве цифре), следеће је локација рођења у Србији (два броја), а након тога редни број рођења у том дану који се разликује према полу од нуле до петсто – мушки и од петсто до хиљаду – женски, последњи број је рачунарски генерисан.[20] Злоупотребе овог податка су незамисливих размера посебно уколико размотримо начин опхођења особља у многим државним органима са овим обликом приватне информације. На пример различити здравствени картони деце у обдаништима, у дому здравља, социјалном Националној агенцији за запошљавање, пореској управи итд. У овоме може да послужи и анализа скорије донетог Закона о тајности података у чијој глави VII у казненим одредбама предвиђено кривично дело чланом 98. Које гласи:[21] Ко неовлашћено непозваном лицу саопшти, преда или учини доступним податке или документа који су му поверени или до којих је на други начин дошао или прибавља податке или документа, а који представљају тајне податке са ознаком тајности „ИНТЕРНО" или „ПОВЕРЉИВО", одређене према овом закону, казниће се затвором од три месеца до три године. Ако је дело из става 1. овог члана учињено у односу на податке означене, у складу са овим законом, степеном тајности „СТРОГО ПОВЕРЉИВО",казниће се затвором од шест месеци до пет година. Ако је дело из става 1. овог члана учињено у односу на податке означене, у складу са овим законом, степеном тајности „ДРЖАВНА ТАЈНА", учинилац ће се казнити затвором од једне до десет година. Ако је дело из ст. 1. до 3. овог члана учињено из користољубља или ради објављивања или коришћења тајних података у иностранству или је извршено за време ратног или ванредног стања, учинилац ће се казнити за дело из става 1. овог члана затвором од шест месеци до пет година, за дело из става 2. затвором од једне до осам година, а за дело из става 3. затвором од пет до петнаест година. Ако је дело из ст. 1. до 3. овог члана учињено из нехата, учинилац ће се казнити за дело из става 1. овог члана затвором до

[20] Интересантно је овде направити паралелу – већина Американаца (87%) може се јединствено идентификовати на основу датума рођења, петоцифреног поштанског броја и пола (Malin, B. (2005) Betrayed by my shadow: Learning data identify via trail matching, *Journal of Privacy Technology*, June 2005).

[21] „Сл гласник бр. 104/09" из децембра 2009. год.

две године, за дело из става 2. затвором од три месеца до три године, а за дело из става 3. затвором од шест месеци до пет година.

IV) РЕАЛНОСТ

Постоји велики проблем што се у Србији, овако описана информација не третира ни као податак са ознаком интерне ни као податак са ознаком службене или било какве друге тајне. Са друге стране можемо имати следећу ситуацију, (иста је из животног случаја једног од аутора овог чланка) у којој се према интерним правилима одређене институције неки подаци, веома рестриктивно користе, да иду чак до следећих граница. Приликом аплицирања за продужетак дозвољене позајмице текућег рачуна (који се третира као кредит) неопходно је да банка прималац захтева за продужење добије позитиван извештај кредитног бироа за захтеваоца – физичко лице. Оно што је најстрашније за такав упит код кредитног бироа неопходан је пристанак клијента, а онда следи једно велико изненађење, након тога што сте ви дали свој пристанак да један (било који чиновник одређене банке – јер није неопходно да са тим чињеницама и информацијама баратају посебно обучена лица) радник дате институције оствари увид у скоро целокупан живот одређеног лица (у питању су укупни приходи и расходи, кредитна задуженост и оптерећење одређеног лица као и одређење његових кредитних јемаца – жираната или постојећих хипотека и ко зна све чега још) Ви немате право да добијете примерак оваквог извештаја. Овај моменат је круцијалан, и поред Вашег писменог пристанка да се овакав извештај прибави из кредитног бироа, Ви нисте квалификовани да га прегледате или у било ком облику поседујете! Наравно, овај горе објашњени радник, има и могућност да вишеструко злоупотреби овакве податке – од типовања за неко имовинско кривично дело до уцењивања због постојања прикривених фондова.

V) ЗАКЉУЧАК

Све наведено сада може бити искоришћено у једној фикцији – замислимо у једној значајној теорији завере (коју бисмо могли одредити као један криминалистички модел) да се многи користе најразличитијим средствима за прибављање информација о одређеним лицима, како би на један најпростији начин злоупотребили ове податке. О вама делове информација једна особа (извршилац крађе идентитета) може прибавити најглобалније податке са неке од поменутих онлајн социјалних мрежа (уколико прогутамо фикцију о ограничавању дистрибуције приватних

података а што је тешко због могућег коришћења краулера и такозване временске машине).[22] Након овако прикупљених података у нашој фикцији долазимо до момента који је релативно значајан за извршиоца, даљи продор и повезивање информација може бити коришћен за даљу продају на Интернету кроз базе података који су на овај начин прикупљени уз додатне информације о обављеним електронским трговинама као и најразличитије идентификационе информације за обављање трансакција – дакле уз комбиновање превара са кредитним и платним картицама. Наравно могуће је и да се ови подаци користе на неки од следећих начина, кроз личне интеракције и покушаје злоупотребе прибављених информација путем уцене због постојања одређених компромитујућих фотографија по мету или могуће злоупотребе ових информација у циљу класичне крађе идентитета и уз временско одложено злоупотребљавање таквих информација (дакле не кроз креирање фиктивних идентитета, већ злоупотрбу постојећих). Колико су ова средства полуге осамљивања човека у оваквом свету хипер комуникације, а колико она представљају средства која огољавају човека и његов социјални круг за неке непозване госте у ову врсту интиме? Наиме, прво човек у оваквим околностима све облике комуникације остварује у оквирима ових социјалних релација па, на послетку, није у потреби да се излаже другим типовима комуникације. Овако замишљено матрикс окружење може водити потпуном затварању човека и губљењем потребе да се оствари физички контакт. Са друге стране, могуће је и да се на овај начин олакшава посао одређеним структурама обавештајних служби о препознавању социјалних контаката и веза одређене особе. Наиме оно што је чинило веома недоступан круг или чак систем за многе обавештајне службе, и што је било сан оперативаца, сада је доступно на дохват руке. Само је неопходно да неки хакер упадне у систем ових социјалних мрежа и ето свих контаката особе на длану. Овде се прича не завршава, веома значајно је размотрити и могућности коришћења ваших персоналних докумената и фото и видео записа истакнутих на Интернету управо уз помоћ ових web 2.0 апликација. У пракси је веома учестао облик коришћења приватних и личних садржаја са Интернета на забрањен начин а, неретко, од стране сексуалних предатора и што је нарочито опасно педофилских сексуалних предатора.

[22] Могуће је преко овог средства вратити се у прошлост према веб страницама и са различитих тренутака у времену преузети комбинације података које до одређеног тренутка нисмо прикрили, осим у претпоставци да смо такве податке од првог момента на социјалној мрежи сакрили за ширу јавност.

Ово посебну димензију добија када посматрамо феномен социјалних мрежа и истицање најразличитијих фотографија (деце, обнажене деце на купању на мору, и томе слично). Све описано даје само једну широку диспозицију у којој су на удару скоро сви актери на вебу: од малолетне деце до старијих лица, извршиоци су такође веома различити и веома им је доступна анонимност, могућност прикривања и искоришћавања погодности удаљених локација, интернационалне димензије и многа друга средства која нису на располагању обичном криминалцу у реалном свету. Према интерполовим сазнањима најразличитији су облици превара путем Интернета, од којих се и на нашим просторима јављају неке (које су већ значајно присутне у другим деловима света):

1. Преваре путем Интернета у разним видовима нпр. „добици" на Интернет лутрији, обично понуде стигну са адресе из Велике Британије или из Холандије. Потребно је само уложити хиљаду-две британских фунти, па да се шатро активира девизни рачун на који ће да буде уплаћен добитак од милион фунти. У последње време јако је актуелна лутрија светског купа у Јужној Африци.
2. Молба за улагање у рад политичке партије у Нигерији или за помоћ повратку VIP особе која је прогнана или је у бекству из своје државе и крије се у некој трећој држави, а баш би са твојим новцем вратила правду, ред и поредак, у некој афричкој држави (обично се ради о државама у којима је тренутно стање после државног удара или војног пуча и сл.). У типологијама ИЦЗ ова превара се назива инвестиционим преварама и као ужу групу има преваре са плаћањем унапред.
3. Међународно пружање адвокатске помоћи и понуда за паушално плаћање такве помоћи. Наравно, адвокат је нпр. неко из Кеније или Нигерије, а баш случајно живи и ради у Холандији или Великој Британији. Као што се може закључити и ово је вид преваре са исплатом унапред.

Када се овакви случајеви проверавају са надлежним службама Велике Британије и Холандије посредством ИНТЕРПОЛ-а, одговор је увек исти: адресе не постоје, адресе постоје али се на њима налазе фабричке хале или стоваришта, власници/корисници фиксни односно мобилних телефонских бројева не могу бити утврђени или су дати телефонски бројеви неких јавних служби или музеја и сл. Наведена имена контактособа не пролазе евиденције грађана и највероватније су измишљена. Начин супростављања овој групацији зависи од системске позиције, наиме немогуће је свакој од наведених угрожених група другачије прићи, а

немогуће је и дејствовати линијски по сваком од извршилаца у сваком тренутку. Као једно од могућих решења издваја се могућност да се на стратешком нивоу поставе одређене безбедносно базиране политике и да се уз сарадњу са приватним сектором и јавношћу предупређују овакве ризичне диспозиције. Превенција се може огледати у едукацији приватних корисника као угрожених група, али и едукацији и успостављању нових пословних политика у државним органима и другим могућим метама извршилаца крађе идентитета. Један од могућих случајева покушаја давања адекватног одговора на овај облик криминалитета јесте адекватно инкриминисање крађе идентитета као кривичног дела а са друге стране и дејствовање у области заштите личних података на пример увођењем новог другачије формулисаног идентификационог броја грађана.

VI) ИЗВОРИ

- Dwyer, C. (2007) "Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study.
- Coppola, N., S. R. Hiltz, and N. Rotter (2004) "Building Trust in Virtual Teams," IEEE Transactions on Professional Communication (47) 2.
- Malin, B. (2005) Betrayed by my shadow: Learning data identify via trail matching, Journal of Privacy Technology, June 2005.
- Mayer, R. C., J. H. Davis, and F. D. Schoorman (1995) "An Integrative Model of Organizational Trust," The Academy of Management Review (20) 3.
- Metzger, M. J. (2004) "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce 9 (4)," Journal of Computer-Mediated Communication (9) 4.

Интернет извори:

- www.wikipedia.org\web2.0
- http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/
- http://facebook-uses.questionpro.com/
- http://www.facebook.com/terms.php?ref=pf
- http://www.facebook.com/policy.php
- http://www.youtube.com/watch?v=wrnYRPRF36E&feature=player_embedded# http://www.revija92.rs/code/navigate.php?Id=599&editionId=50&articleId=217.