SZOMMER Károly – BALOGH Zoltán – RACSKÓ Péter

AZ ON-LINE VILÁGBAN HAGYOTT VIRTUÁLIS LÁBNYOMOKBAN REJLŐ INFORMÁCIÓK ÉS AZOK VESZÉLYEI

A mindennapi, szinte folyamatos jelenlét a hálózaton számos melléktermékkel jár. Minden bejelentkezés, üzenet, vásárlás, akció adatok tömegét hagyja az interneten. A cikkben arra kívánnak a szerzők rámutatni, hogy ezeket az adatokat valaki vagy valakik összegyűjthetik, és esetleg olyasmire is használhatják, amihez nem járulnánk hozzá, ha ezt megkérdeznék. A szerzők nem foglalkoznak a rosszindulatú, esetleg bűntények elkövetésének céljára történő illegális adatgyűjtéssel, illetve -hasznosítással, azt kívánták bemutatni, hogy teljesen legális, ún. „white hat" eszközökkel is tartalmas felhasználói profilt lehet összeállítani. Szót ejtenek arról is, hogyan lehet megnehezíteni azok dolgát, akik rólunk szeretnének információt gyűjteni.

Kulcsszavak: **virtuális lábnyom, személyes adatok, adatvédelem, geotagging, mobilszolgáltatás**

Bármerre is járunk, legyen szó bevásárlásról, utcai sétáról, utazásról, pénzügyeink intézéséről vagy egyszerű internetezésről, „digitális lábnyomunkat" szinte mindenütt magunk mögött hagyjuk. Ennek mértéke átlagosan személyenként 27 MB naponta (Túri, 2011). Ezeket az adatokat az internetes oldalak felépítésének ismeretében egy egyszerűbb adatgyűjtő program, ún. crawler segítségével könnyen össze lehet gyűjteni és a továbbiakban felhasználni (Szommer, 2013). Mindenkiben felvetődik a kérdés, hol és milyen módon hagyunk hátra adatokat? Össze lehet-e gyűjteni a különböző helyeken és alkalmazásokban rólunk hátrahagyott adatokat? Hogyan lehet a nem kívánt adatgyűjtés ellen (legalább részben) védekezni? Megérik-e a kapott szolgáltatások azt, hogy adatainkat szétszórjuk az interneten? A válaszokhoz először meg kell vizsgálnunk a digitális lábnyomok természetét.

A digitális lábnyomunk számunkra vagy egy átlagos felkészültségű, legálisan működő harmadik fél számára is nagyrészt hozzáférhetetlenek. Nem férünk hozzá a biztonsági kamerák felvételeihez, telefonhívásaink és bankszámlaműveleteink számítógépes naplóihoz, vagy az általunk megtekintett tartalmak egyébként részletes naplóihoz. Vannak viszont olyan adatok, amelyeket szándékosan teszünk közzé – korlátozottan vagy korlátozás nélkül – képek, videók, önéletrajzunk stb. Az adatok jelentős része internetes aktivitásunk során keletkezik anélkül, hogy tudnánk róluk. Adataink tárolását az alábbi négy paraméter jellemzi (Túri, 2011):

- tárolási idő: mennyi ideig őrzik meg az adatot?
- érzékenység/bizalmasság: milyen mértékben befolyásolja az adat későbbi előkerülése a nyomot hagyó viselkedését?
- hozzáférhetőség: nyilvános vagy magánadatbázisban kerül tárolásra, kinek lesz hozzáférése az adott adathoz?
- tudatosság: a felhasználó az adatok rögzítésével kapcsolatos ismeretei.

A rólunk összegyűjtött adatokat mások felhasználhatják saját céljaikra, például célzott marketingtevékenységre. Erre jó példa a McDonald's egyik akciója, amellyel a mobilozó fiatalságot célozta meg: öt- és tízdolláros ételutalványokat sorsoltak ki azok között, akik a geográfiai helyzeten alapuló kapcsolatokat támogató közösségi oldalon, a FourSquare-en bejelentkeztek egy McDonald's étterem közeléből (Slovak, 2012). Az internetes hirdetések sokszor hasznosak is lehetnek. Ennek azonban ára van, amennyiben olyan személyek kezébe kerülnek adataink, akik azokat rossz

célokra használják fel, a dolog vége lehet akár betörés, emberrablás vagy személyiséglopás is. A cikkben azt mutatjuk be, hogy törvényes úton, előzetes engedélykéréssel vagy anélkül, mennyire könnyű információt szerezni konkrét személyekről. Azt az olvasó ismereteire és fantáziájára bízzuk, hogy ezekkel az adatokkal hogyan lehet visszaélni. Nem tárgyaljuk az illegális, törvénytelen információszerzési módszereket és ezek hatásait, ehhez elég olvasni a napi sajtót.

Hogy juthatunk többletinformációhoz a felhasználókról?

Többféleképp kaphatunk információt a felhasználókról:

- egyszerűen engedélyt kérünk a felhasználó profiljához való hozzáféréshez, vagy valamilyen módon motiváljuk őket (például nyereményjátékkal), adataik megosztására,
- illegális módon, megtévesztéssel bekerülünk a felhasználó „belső információs köreibe", majd célzottan átböngésszük az így hozzáférhetővé vált tartalmat,
- olyan technológiák megfelelő ismeretében, amelyeket a felhasználó nem ismer eléggé, de mégis használja, és így tudta nélkül több információt hagy maga mögött, mint amit szeretne.

Jelen cikkben a fenti technikák közül kettőt ismertetünk egy-egy valós példával, eredményeikkel és veszélyeikkel együtt: az engedélykéréssel szerzett információval kapcsolatos, valamint a technológiai ismeretkülönbséggel szerzett információval kapcsolatos terület.

Az engedélykéréssel szerzett információ

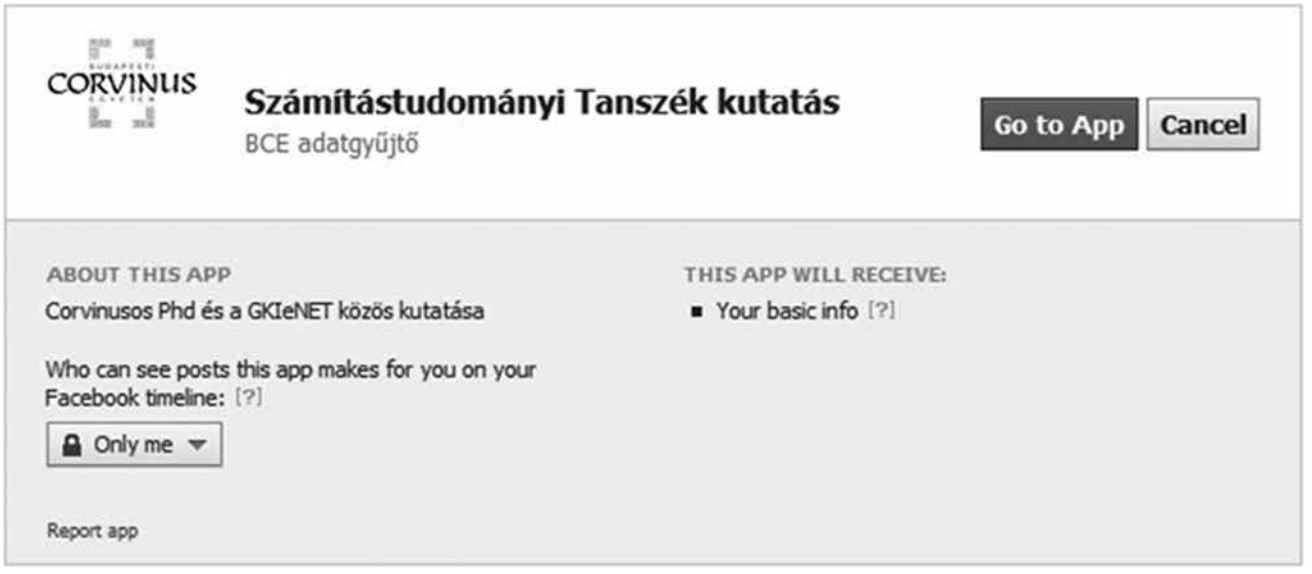
Az első eset, amelyet bemutatunk, egy 2012. áprilisi kutatás leírása. A kutatás során a Budapesti Corvinus Egyetem e-learning rendszerében egy hónapig működő adatgyűjtő programot helyeztünk el a felhasználók beleegyezésével. Az alkalmazás *(1. ábra)* a látogatók minden, szerveroldalról hozzáférhető adatát elmentette. Továbbá, ha a látogatók a hozzájárulásukat adták, elmentette a Facebookon található adataikat és a földrajzi pozíciójukat is. A kutatás azt vizsgálta, hogy milyen információt nyerhetünk ki az oldal látogatóiról, a felhasználók ennek mennyire vannak tudatában, és tesznek-e ellene egyáltalán. A kutatást két részre osztottuk.

Az első két héten az adatok megosztása önkéntes alapon történt. Ekkor mindennemű lehetséges nyeremény nyújtása nélkül folyt a kutatás. Az utolsó két héten nyereményjátékkal ösztönöztük a felhasználókat, hogy minél több információt megosszanak magukról. A nyeremény az időszak végén 30 darab, 2 GB-os MicroSD-kártya volt, amit azok között sorsoltunk ki, akik megosztották az adataikat.

Az e-learning rendszernek összesen 8542 regisztrált felhasználója volt a kutatás ideje alatt, amiből 8466 lépett be. Ez a szám az egyetem tanárainak és diákjainak megközelítőleg a felét jelenti. A kutatás első két hetében 76 felhasználó engedélyezte az adataihoz való hozzáférést, 264 esetben engedélyezték a földrajzi pozíciójukat és 268 879 rekordot rögzített az alkalmazás. Ezzel szemben az utolsó két héten a nyereményjáték alatt 139 felhasználó engedélyezte a Facebook adatlapjához való hozzáférést, 303 esetben adták meg a földrajzi pozíciójukat és 647 298 rekordot rögzített az alkalmazás.

1. ábra

A kutatáshoz készített Facebook-alkalmazás



A kutatás után a nyereményjáték nyerteseivel kitöltettünk egy-egy kérdőívet, amiben többek között arra is rákérdeztünk, hogy ismerik-e azt a lehetőséget a Facebookon, amivel vissza lehet vonni a jogosultságot külső alkalmazásoktól. A kérdőívet kitöltők 89,6%-a úgy nyilatkozott, hogy ismeri a külső alkalmazások jogosultságának visszavonásának lehetőségét, és használják is.

Az aszimmetrikus technológiai ismeretekkel, engedélykérés nélkül szerzett információ

Egy másik módja az információszerzésnek az, amikor technológiai ismereteinket használjuk fel a többletinformáció megszerzéséhez. Erre tipikus példa a geotagging módszere, ami a felhasználók számára megkönnyíti az elkészített képek, videók GPS-koordinátával való címkézését (automatikussá teszi ezt). Ezt követően a publikálás során lehetőségük van azokat egy térképen is szemléltetni, így egy külön lehetőségük nyílik a rendszerezésükre is. A többi felhasználó a térkép megfelelő részeihez fűzött képek segítségével könnyebben megismerheti az adott környéket, megtekintheti a környékbeli nevezetességeket.

Egyre inkább terjed az a szokás, hogy amit lefényképezünk a telefonunkkal, azt másokkal megosztjuk valamilyen formában az interneten. A képformátumok nagy része rendelkezik egy Exif fejléccel, amely többek közt tárolja a képet készítő gép adatait és a kép készítési helyszínének pontos földrajzi koordinátáját is (TsuruZoh, 1999). Miközben a felhasználó a képeket publikálja, a legtöbb esetben nincs tisztában azzal, hogy nemcsak a megjelenítési információkat teszi közzé, hanem többek közt azt is, hogy adott időpillanatban ő hol is tartózkodott. Ezt a technológiát olyan mértékben hagyják figyelmen kívül, hogy ha megnézzük a telefonokat forgalmazó cégek weboldalait, kevés helyen találunk információt arról, hogy egy adott készülék képes-e a képek földrajzi koordinátákkal történő felruházására vagy sem. A képek földrajzi koordinátákkal való összekapcsolását nevezzük geotaggingnek, a képhez tartotó földrajzi adatokat pedig geotagnek.

Aki nem ismeri ezt a sokszor automatikusan alkalmazott technológiát, az a képek megosztásával különböző veszélyeknek teheti ki magát: felfedheti esetleg titkolt tartózkodási helyét (Murphy, 2010), gyermekmolesztálók figyelhetik meg a kisgyermekek mindennapi haladási útvonalait (Tonder, 2011) stb.

Kétféle módon lehet elkerülni a kellemetlenségeket:

- felhasználói oldalról történő beavatkozással, a készülékek geotagging funkciójának kikapcsolásával, vagy a képekből az információ utólagos kitörlésével, ez a felhasználó dolga,
- szerveroldalról történő beavatkozással, a képek feltöltése utáni Exif fejléc eltávolításával, ez a szolgáltató feladata.

Az on-line képmegosztás során sok esetben sokáig elérhető marad a képekben tárolt geográfiai információ. Ezeket az oldalakat két csoportba sorolhatjuk: az egyik a *közösségi oldalak*, a másik a *csak képmegosztással foglalkozó weboldalak*.

A közösségi oldalak

A következőkben bemutatjuk, hogy a közösségi oldalak mennyire foglalkoznak a geotagging használatával, és annak felhasználói oldalról történő visszanyerhetőségeivel. A vizsgálat nem terjed ki az összes létező közösségi oldalra, csak a legismertebbekre.

A legnépszerűbb közösségi oldal, amely ma már több mint egymilliárd (Donna, 2013) felhasználóval rendelkezik világszerte, a Facebook. Hatalmas népszerűségének köszönhetően a vizsgálat szempontjából kiemelten fontos. Bár a közelmúltban még egyáltalán nem figyeltek oda a GPS-adatok kezelésére, szerencsére mára már megszüntették ezt a veszélyforrást, és csak önkéntesen adható meg földrajzi pozíció a készített képekhez, az is csak pontatlanul.

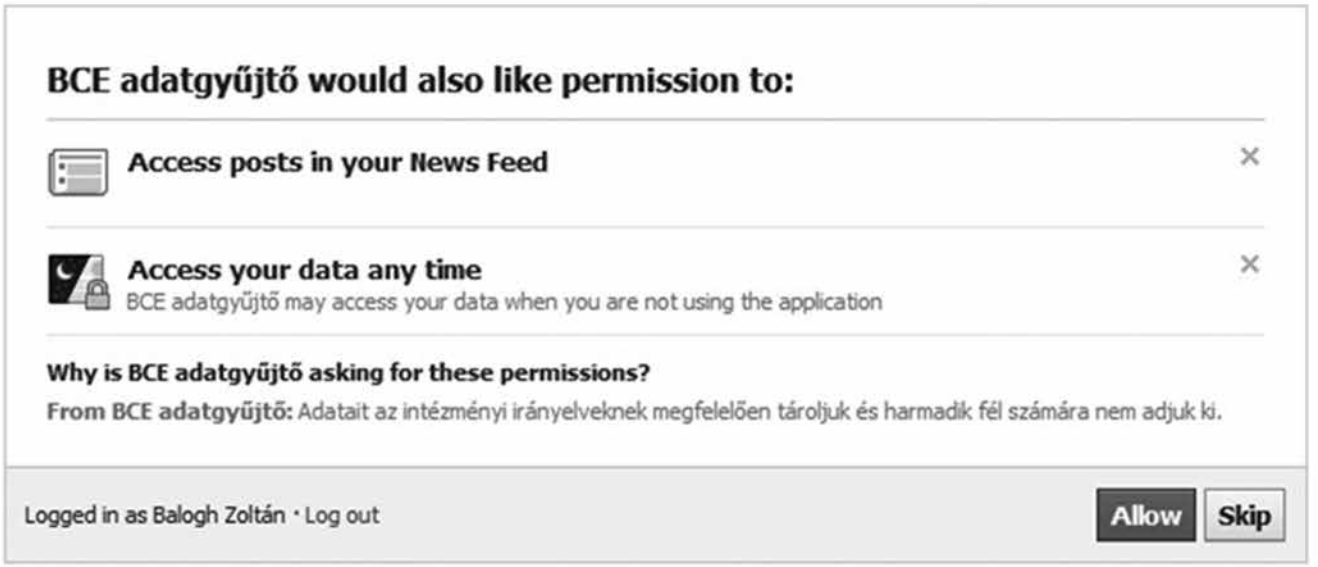
A Google+ támogatja és használja is a geotageket. Ez meglepő felfedezés volt, mivel a Google 2012. március 1-jén változtatta meg adatvédelmi irányelveit, ami után a jóhiszemű fogyasztók azt hihetik el, hogy a Google igenis figyel a különböző technológiai és egyéb változásokra, ráadásul a geotagging mint technológia már számos éve létezik a piacon, és egyre inkább terjed azzal, hogy az okostelefonokon legtöbbször már alapértelmezett beállításként be is van kapcsolva. Tehát a Google+ közösségi oldalon a képekhez tartozó metaadatok mentésre kerülnek, és mindenféle művelet elvégzése nélkül egy egyszerű Exif olvasó kiegészítővel már magán az oldalon megtekinthetők a geotagek.

Ami miatt ez pluszkényelmetlenséget és hatalmas veszélyt is jelent az az, hogy a Google+-on nemcsak a barátaink láthatják megosztott tartalmainkat, hanem bárki, aki hozzáad minket a köreihez. Tehát ha egy nem tudatos felhasználó nem vigyáz arra, hogy kivel osztja meg a tartalmat, akkor tulajdonképpen bárki hozzáférhet a képein lévő GPS-koordinátákhoz.

Semelyik más, általunk vizsgált közösségi weboldal nem támogatta a geotagek megjelenítését, még úgy sem, hogy ahol lehetett, ott a legalacsonyabbra vettük az adatvédelmi beállításokat (*1. táblázat*). Több módszerrel is megpróbáltunk a GPS-koordinátákat megőrizni és visszanyerni, de egyik sem működött. Tehát megállapítható, hogy ezek az oldalak nem támogatják a GPS-koordináták visszanyerését.

2. ábra

Az adatgyűjtő által kért engedélyek ablaka



1. táblázat

A közösségi oldalak elemzése geotagging szempontból

Közösségi oldal neve	URL	Képeken lévő GPS-metaadatok megjeleníthetők
Facebook	www.facebook.com	nem
Google+	plus.google.com	igen
Hi5	hi5.com	nem
iWiW	iwiw.hu	nem
MySpace	www.myspace.com	nem
Netlog	hu.netlog.com	nem
Orkut	www.orkut.com	nem
Twitter	twitter.com	nem

A képmegosztó oldalak

A következőkben a képmegosztó oldalakról adunk átfogó képet a geotagging szempontjából. A vizsgálat nem terjedt ki az összes létező képmegosztó oldalra. Az elemzés során csak a nagyobb forgalmúakat vizsgáltuk.

A Fotolog feltöltés után tömöríti a képeket, ez egy lehetséges oka a GPS-adatok elvesztésének. Ez volt az egyetlen olyan képmegosztó oldal, amely nem támogatta a geotagek megjelenítését.

Az elemzések során a Flickr rendelkezett a legjobb megoldással a témában, nem mellesleg a Picasa mellett ez a legnépszerűbb ilyen oldal. Magukat a GPS-es metaadatokat tárolta, azonban többszöri próbálkozás ellenére sem lehetett azokat kiolvasni egészen addig, amíg jóvá nem hagytuk a képeknél a geotag használatát. Még úgy sem működött, hogy a kép közvetlen URL-jét vizsgáltuk, így elmondható az, hogy a Flickr tartotta legjobban szem előtt a GPS-es metaadatok veszélyét. Népszerűségét mutatja az is, hogy számos, a fényképező eszközökhöz csatlakoztatható GPS-es kiegészítő alapvetően kompatibilis volt már a Flickr-rel, ezért is fontos a megfelelő védelem a szolgáltató részéről. A Photobucket és a Picasa semmiféle védelemmel nem rendelkezik ezen a területen, mindenféle egyéb műveletek elvégzése nélkül mindkettőn könnyedén meg lehet tekinteni a GPS-es metaadatokat. A Picasával a Google második szolgáltatása bukott el a teszten (*2. táblázat*).

2. táblázat

A képmegosztó oldalak és a geoinformációk megjeleníthetősége

Képmegosztó oldal neve	URL	GPS-meta-adatok megjeleníthetőek
Flickr	www.flickr.com	igen
Fotolog	www.fotolog.com	nem
Photobucket	photobucket.com	igen
Picasa	picasa.google.com	igen

Az adatmegosztás tudatosságának mérése

Megvizsgáltuk, hogy az e-learning rendszerben történő kutatás, valamint a geotagginggel kapcsolatos kutatás esetében mennyire voltak tudatában a felhasználók a többletinformáció-szolgáltatásnak, továbbá azt is, hogy ténylegesen mennyire vigyáznak a személyes adataikra.

Engedélykéréssel szerzett adatok esetén

Az e-learning rendszerben történő kutatás során a 30 nyertes személy a MicroSD-kártyák átvételekor egy-egy kérdőívet töltött ki, amelyben többek között arra is rákérdeztünk, hogy figyelnek-e arra, hogy milyen alkalmazásnak adnak engedélyt az adataikhoz való hozzáféréshez. A Facebook felületén felugró engedélykérő ablak a *2. ábrán* látható.

A kérdőívet kitöltők egytől ötig terjedő skálán értékelték informatikai tudásukat. Hármasnál rosszabb értéket senki nem adott magának, az átlag 3,48 lett. Meg kell jegyeznünk, hogy a válaszadók 82%-a nem informatikai szakon tanul. A válaszadók vagy a nyereményjátékot, vagy a kutatás elősegítését jelölték meg adatmegosztásuk okaként. A válaszokból kiderült, hogy a felhasználók bíznak a Budapesti Corvinus Egyetem adatvédelmi szabályzatában és eljárásaiban, és feltételezik, hogy a szabályzat megakadályozza, hogy az adatok illetéktelen kezekbe kerüljenek, valamint úgy gondolták, hogy ha az adatgyűjtő alkalmazást az illetékesek engedték beépíteni az e-learning rendszerbe, akkor az valószínűleg megbízható.

A felmérés egyik legérdekesebb részének tekinthető az a kérdés, amikor arra kellett válaszolni, hogy tudják-e, hogyan kell a Facebookon az alkalmazásoktól visszavonni a jogosultságot. A válaszadók 92,5%-a nyilatkozott úgy, hogy ismerik ennek a módját.

A kutatás után négy hónappal megvizsgáltuk, hogy hányan vonták vissza a hozzáférést a korábban megadott adataikhoz. Azt a figyelemre méltó eredményt kaptuk, hogy a felhasználók 82,4%-a nem vonta vissza a jogosultságot, tehát az adatok továbbra is elérhetők maradtak. A fenti négy hónapban a felhasználókat folyamatosan nyomon lehetett volna követni, és olyan információhoz juthattunk volna, amelyhez korábban ők adták meg a jogosultságot. Nem szüntették meg az azokhoz való hozzáférést annak ellenére, hogy azt nyilatkozták, tudják, milyen módon lehet azt megtenni.

Aszimmetrikus technológiai ismeretekkel szerzett információ

2012 év elején egy on-line kérdőív segítségével felmértük a geotagging használatának tudatosságát. Ezt azért tartottuk fontosnak, mert nagy biztonsági kockázatokat rejt magában a technológia nem körültekintő használata. A kérdőívezést a hallgatók között végzett véletlen mintavétellel végeztük, összesen 210 választ kaptunk. A kérdőívezési módszertant A marketingkutatás alapjai című tankönyv (Simon Judit, 2011) szerint alkalmaztuk.

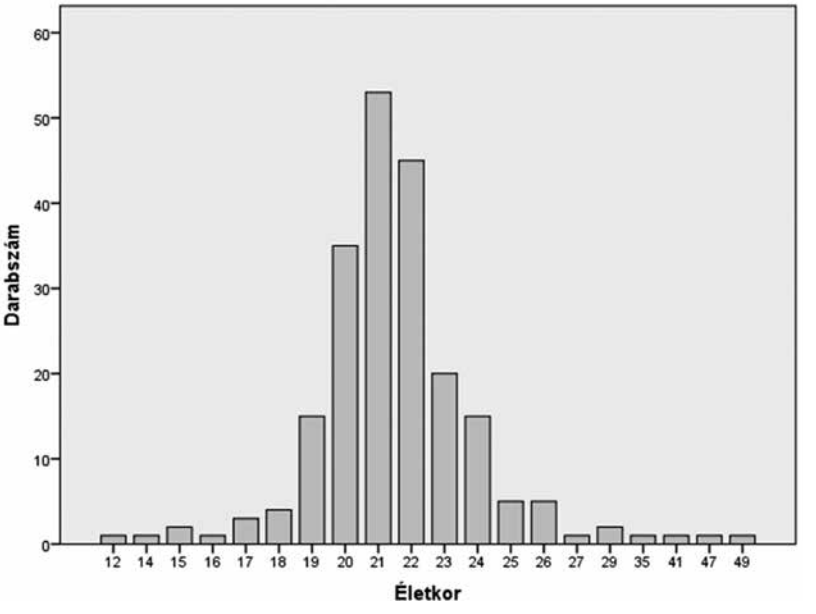
A kérdőív összesen 16 kérdésből állt, a válaszokat listából kellett kiválasztani, így a kitöltés nem vett többet igénybe, mint 5-7 perc. A demográfiai részt a kérdőív végén szerepeltettük, ugyanis akkorra azt már nagyobb bizalommal töltik ki az emberek. A kérdőív szerkesztésekor kerültük az irányított és a túlzottan személyes kérdéseket, hogy ezzel is növeljük a kitöltési hajlandóságot.

A felmérés országos viszonylatban nem tekinthető reprezentatívnak a demográfiai megoszlás miatt. A kitöltők 62%-a (129 fő) volt budapesti lakos, 63%-a (133 fő) jelenleg is a felsőoktatásban tanul. Az adatok ugyanakkor jelzésértékűek és egy későbbi felméréshez kiindulási alapul szolgálhatnak. A kitöltők átlagéletkora 22 év volt. A legfiatalabb válaszadó 12, míg a legidősebb 49 éves volt. A kitöltők átlagos életkora 21,77 év volt.

A demográfiai sajátosságok (*3. ábra*) mutatják azt, hogy a minta nem reprezentálja az ország lakosságát, ugyanakkor a lefedett populáció a geotagging szempontjából a legjobban érintett. Maga a geotagging korszerű informatikai eljárás, és feltételezhető, hogy az idősebb és a relatíve fiatalabb (12–18 éves) korosztályok e tekintetben a kevésbé tudatos felhasználók közé tartoznak. A felmérésben ezek a korosztályok alulreprezentáltak, így feltételezhető, hogy egy ténylegesen reprezentatív mintán alapuló kutatás során sokkal rosszabb adatokat kapnánk a tudatos használatban.

3. ábra

A geotagging kérdőívet kitöltők életkorának megosztása



Még jelenleg is sokan választanak úgy telefont, hogy nincsenek tisztában a készülék főbb funkcióival, így tőlük aligha várható el, hogy tudatosan figyeljenek arra, hogy a készülék elhelyez-e automatikusan geotageket a fényképeken, vagy sem. A válaszadók 36%-a jelezte, hogy a készüléke képes geotaggelésre, 35%-nak pedig nem volt tudomása erről. 29% szerint a készüléke nem képes geotaggelésre, ám az ilyen válaszokat ellenőriztük. Kiderült, hogy nagyon sok olyan kitöltő is így nyilatkozott, akinek a készüléke minden kétséget kizáróan képes geotaggelésre. Mivel ez a funkció legtöbbször a telefonok alapbeállításai szerint be van kapcsolva, az ismeretek hiánya a készülékek tulajdonosai számára kockázatot jelent.

A válaszadók 46%-ának nem volt tudomása arról, hogy ezeket a metaadatokat meg lehet tekinteni mélyebb informatikai tudás nélkül is a geotaggelt képeken, továbbá a válaszadók 44%-ának még ez eddig nem is jutott eszébe, hogy mások visszaélhetnek ezekkel az adatokkal.

A digitális dosszié

Az interneten magunk mögött hagyott adatok összegyűjtésével, a digitális nyomok összességéből össze lehet állítani egy ún. digitális dossziét, amely egy helyen, integráltan tartalmazza egy személy a legkülönbözőbb helyeken elszórt adatait. A digitális dosszié annyira teljes, amennyire a dosszié összeállítója technikailag képes összegyűjteni az interneten szétszórt adatokat. Az interneten hagyott adatok jelentős része természetesen nem érhető el nyilvánosan. Például a webes boltok üzleti titokként őrzik vásárlóik adatait, a közösségi oldalak nem teszik hozzáférhetővé a nem megosztott adatokat, az egészségügyi intézmények gondosan őrzik orvosi leleteinket stb. (Daniel, 2002).

Potenciális digitális dossziénk már az első ultrahangképpel, még születésünk előtt elkezd íródni, és a folyamat még a halálunkkal sem fejeződik be, gondoljunk csak a különböző emlékoldalakra. A köztes időben pedig mi magunk vagyunk elsősorban azok, akik valamilyen módon megosztjuk adatainkat. Használjuk a hűségpontokat gyűjtő kártyákat, közzéteszünk különféle digitális tartalmakat, regisztrálunk webhelyekre, ahol ismét megadjuk adatainkat. Elsétálunk a térfigyelő kamerák előtt is, melyek felvétele rögzítésre kerül, amit esetleg ki is elemeznek valamilyen szoftver segítségével (Reardon, 2012). Nyilvános adatból is, főleg a nem tudatos internethasználat mellett, rengeteget osztunk meg. Ehhez adódnak hozzá a kötelező adatszolgáltatások: munkahelyünk honlapján kötelezően megadott önéletrajz, nyilvánosan megjelenő sporteredmények, az üvegzsebtörvény előírásainak megfelelő adatok stb.

Amennyiben egy-egy személy adatait huzamosabb ideig tudjuk követni, és azt meg is tesszük, az általa hátrahagyott digitális lábnyomokat feljegyezve vaskos digitális dossziét állíthatunk össze. Ez már nemcsak egy pillanatkép, hanem az adott személy élettörténetét is valamilyen pontossággal tartalmazza. Az élettörténet elemzésével sok olyan információt deríthetünk ki, amit máskülönben csak egy pszichiáter, vagy a személy közvetlen környezete ismerhet.

A személyes adatok értéke

Emberek százmilliói használják az interneten található „ingyenes" szolgáltatásokat, amiért lényegében a személyes adataikat adják cserébe, azaz azzal fizetnek. A magánélethez való jog alapvető emberi jog. Az internet és a széles körben használt közösségi oldalak miatt sokakban felmerül a kérdés a magánélet újraértékeléséről és újraértelmezéséről. Véleményünk szerint a személyes adatok védelmében az internet fejlődéséhez képest a világ igencsak lemaradt.

Az Európai Unióban az Adatvédelmi Direktíva (95/46/EC) rendelkezik a személyes adatok gyűjtéséről és tárolásáról az Európai Unió területén belül, valamint a személyes adatok más országba való átviteléről is, ennek korszerűsítése most van folyamatban. Az EU magánéletet és az emberi jogokat védő törvényei nemcsak az állam, hanem más személyekkel és szervezetekkel szemben is védik a személyes adatokat.

Az internet széles körű felhasználása miatt azonban nagyon időszerű ezeket a jogszabályokat újragondolni, ugyanis a személyes adatok jelenleg a piacon lévő igen értékes, ha nem a legértékesebb, árucikkek. A Facebook IPO-ja és más közösségi oldalak részvényeinek értéke bizonyítja, hogy a személyes adatok többé már nemcsak emberi jogi kérdések, hanem igen szignifikáns üzleti értéket is jelentenek. A már meglévő adatokat, ha kiegészítjük a nyílt internetről összeszedett további releváns adatokkal, még nagyobb információvagyonra tehetünk szert.

Az esetek legnagyobb részében a felhasználók az „ingyenes" szolgáltatásért cserébe tehát személyes adataikat adják. Ezzel kapcsolatosan feltehetjük a kérdést: „ki a nyertes ebben a cserében?" és „használhatjuk-e a személyes adatainkat fizetőeszközként?"A személyes adatok csereértékének elemzésében az aszimmetrikus információ szerepét kell vizsgálni.

A legtöbb felhasználó nem érti, hogy személyes adatai jelentős értékkel bírnak a szolgáltató számára és ezért önként odaadják azokat. A szolgáltatók az adatok használatából finanszírozzák működésüket, az „ingyenes" szolgáltatásaikat, és emellett profitot is termelnek.

Ezek után tehát nyilvánvaló, hogy a személyes adataink üzleti értéke van. A felhasználók legnagyobb része ezzel a ténnyel nincs tisztában, és „áron alul" adja oda személyes adatait.

Legtöbbször a szolgáltatások igénybevételéhez a felhasználónak el kell fogadnia a cég adatvédelmi szabályzatát. Az adatvédelmi szabályok elfogadásával beleegyezik, hogy a cég használhatja a személyes adatokat az abban leírtak szerint. Ha mégsem kattint az elfogadásra, akkor az adatvédelmi szabályzat megakadályozza, hogy a cég felhasználja az adatokat, valamint a cég is megtagadja a szolgáltatás teljesítését (Kassner, 2012).

Sokszor ezek az adatvédelmi szabályzatok változnak. Michael Kassner azt elemezte, hogy a szolgáltatást nyújtó vállalatok hogyan változtatják meg a sajátjukat (Kassner, 2012), sokszor a felhasználók tudta és kifejezett beleegyezésük nélkül. Paul Ohm ezt a jelenséget az adatvédelmi szabályozás cserbenhagyásának nevezi (Ohm, 2012). Közelmúltbeli példaként a Google 2012-es akciójára gondoljunk, amikor a különböző alkalmazások közötti falat lebontották. Valószínűleg a felhasználók nagy része nem tudta, hogy ez miért is érte meg a cégnek.

Most, hogy látjuk, a cégek óriási fejlesztésekre vállalkoznak a bevételük növelése érdekében, vizsgáljuk meg, hogy miként is kalkulálhatnak a megtérüléssel kapcsolatban. Egy-egy új szolgáltatás indításához viszonylag sok pénzt kell beruházni, és kérdéses, hogy megtérül-e. Nem könnyű egy-egy szolgáltatás jövőben várható nyereségét előre meghatározni annak használata előtt, ha nem ismerjük, hogy a felhasználók mennyit hajlandók érte fizetni a személyes adataikból, továbbá, ha nem tudjuk, hogy milyen típusú felhasználók fogják azt használni.

Az on-line közösségi oldalak bevételének döntő része a hirdetőktől származik. Az egyes felhasználók marketingértéke eltérő lehet a potenciális eladók számára, attól függően, hogy mely országból származnak, milyen korúak, mi a nemük, képzettségük és természetesen vásárlóerejük stb. Egy kevésbé jómódú országból származó felhasználó adata átlagosan kevesebbet ér a hirdető számára, mint egy gazdag országban élő felhasználóé.

Most nézzünk egy példát a felhasználói adatok beárazására. A Facebook tőzsdei bevezetése 2012. augusztus 23-án történt meg, és a Nasdaq-on hivatalosan 41.647.625.600 USD-ért jegyezték, ami részvényenként 19.41 USD-t jelent. A bevezetés után közvetlenül az árfolyam meghaladta a 40 USD-t. Így a közel egymilliárd felhasználóval rendelkező Facebook átlagos ára 50 USD és 125 USD között mozog felhasználónként. A cég könyv szerinti értéke jelentéktelen, ha a piaci értékéhez hasonlítjuk.

A felhasználók védelme az adataikkal való visszaéléssel szemben

Az adatvédelem az internet fejlődéséhez képest jelentős lemaradásban van. Mindenki számára ismerős az az elcsépelt közhely, hogy ami az internetre felkerül, az többé nem törölhető. Ez a kijelentés nagyjából igaz is, bár léteznek olyan cégek, amelyek vállalják, hogy a megbízóik interneten hagyott nyomait eltüntetik. Sajnos ez a szolgáltatás meglehetősen költséges, mert meg kell fizetni az ehhez szükséges szakértelmet és a nem kevés munkaidő-ráfordítást is.

Több mint egy éve, 2012. január 25-én Brüsszelben terjesztették elő azt a javaslatot, ami kimondja, hogy biztosítani kell az adathordozhatóság jogát, a személyes adatok tárolásának megszüntethetőségét, valamint létre kell hozni az adatvédelem egységes európai szabályrendszerét (European Comission, 2012). Az egységes európai szabályrendszer egyelőre még várat magára. Az eddigi szabályozásban rendkívül sok az olyan folt, ami a felhasználókat kiszolgáltatottá teszi az interneten leselkedő veszélyeknek. Ezt a kiszolgáltatottságot nemcsak a kormányzati intézkedések, hanem a tudatos internethasználat hiánya is erősíti.

A felhasználók nagyrészt nem figyelnek arra, hogy mit osztanak meg egymással, valamint azzal sem foglalkoznak, hogy a megosztás technológiailag milyen további veszélyeket hordozhat magában. Ahogy a keresőmotorok fejlődnek, úgy válnak a rég elfeledett, megosztott, apró töredékadatok egyre inkább fellelhetővé. Az interneten évek alatt ottfelejtett információmorzsák végül összeállnak egy teljes egésszé. Így egy-egy személyről sokszor olyan dolgokat is kideríthetnek, amelyeket ő már rég el is felejtett, de ha tudna is ezekről, mindenképp szeretné titokban tartani.

Többféle módszert is megvizsgáltunk, hogy miként lehet megnehezíteni adataink megszerzését, illetve megnehezíteni az azonosításunkat. A felsorolásban a legfontosabbak ismertetése kerül sorra:

- Az első a közösségi oldalak használatának kerülése. Bár a biztonsági beállítások körültekintő konfigurálása után joggal gondolhatnánk, hogy adataink nincsenek veszélyben, ennek ellenére több esetben is előfordult, hogy csalók a felhasználók bizalmába férkőztek, majd felhasználták az adataikat.
- A következő lehetőség a nyomkövető blokkolók használata. Egyes oldalak, ilyen például a Facebook is, még a kijelentkezésünk után is követi, hogy merre járunk, milyen oldalakat nézegetünk (Asher, 2011). A nyomkövető blokkolók (mint például a Ghostery-alkalmazás) kiszűrik a követéshez használt kódokat, és ezáltal nehezebb

meghatározni, hogy mikor, merre is járunk a világhálón.

- A harmadik, de nem utolsó lehetőség a böngészők inkognitó módjának használata. Ez főleg akkor hasznos, amikor több személy által elérhető számítógépről internetezünk. Ennek a funkciónak a használatával a böngésző a merevlemezen semmit nem fog eltárolni az internetezési előzményünkből, így növelhetjük a visszakövethetetlenségünket.

Léteznek kezdeményezések a követhetetlenségre, ilyen a Do-Not-Track-alkalmazás is, amely jelzi a kiszolgálónak, hogy a felhasználó nem szeretné, hogy kövessék. Ez azonban csak egy ajánlás, a kiszolgálóoldalról vagy figyelembe veszik a kérést, vagy nem. A Twitter már adoptálta ezt a technológiát, azonban kevesen foglalkoznak ezzel a lehetőséggel (Matthew, 2012).

Összefoglalás

A XXI. században megkezdődött az új kincsesbányák kitermelése, a felhasználók adatainak tömeges hasznosítása. A hagyományos bányákhoz képest itt a legnagyobb különbség az, hogy ezeket a kincseket mi önként visszük a feldolgozókhoz és „adjuk le", mégpedig azért, hogy egy-egy szolgáltatást igénybe vehessünk.

Sokan nincsenek tisztában ezen adatok értékével, így nagyon könnyen lemondanak róluk, mint azt az e-learning rendszerbeli kutatás is mutatta. Külön figyelmet érdemel az a tény, hogy egy, a mai viszonylatokban már igencsak jelentéktelennek mondható ajándéktárgy megszerzésének lehetősége is milyen elképesztő módon beindítja az adatmegosztási hajlandóságot. Bizonyos információkat olykor nem is szándékosan osztanak meg a felhasználók. A geotagginges kutatással kapcsolatosan elmondható, hogy a tudatos internethasználat és a megfelelő technológiai ismeretek hiánya miatt a felhasználóknak fogalmuk sincs arról, hogy mikor, hol hagynak maguk mögött nyomot, illetve arról sem, hogy ha szándékosan publikálnak is valamit, milyen többletinformációt szolgáltathatnak ki a technológia használatával.

Ez egy nagyon fontos téma mind a felhasználók, mind a szolgáltatást nyújtók, a jogalkotók és a kormányzat szempontjából. Mindenki jobban teszi, ha folyamatosan nyomon követi ezeket a technológiai változásokat, hogy a maga szempontjából megfelelően tudjon lépni a változásokkal kapcsolatban, ugyanis az adatvédelmi szabályozás jelenleg az internet fejlődéséhez képest gyerekcipőben jár. Így egyelőre mindenkinek résen kell lennie, és elsősorban saját magának kell megvédenie az adatait vagy korlátozott, tudatos megosztással, vagy a technológiák tanulmányozásával.

Felhasznált irodalom

Asher, M. (2011): Facebook tracks you even after logging out. Sydney Morning Herald, http://www.smh.com.au/technology/technology-news/facebook-tracks-you-even-after-logging-out-20110926-1ksfk.html (Letöltés dátuma: 2012. szeptember 25.)

Daniel, J. S. (2002): Digital Dossiers and the Dissipation of Fourth Amendment Privacy. Southern California Law Review, 75: p. 1084–1148.

Donna, T. (2013): CNET. http://news.cnet.com/8301-1023_3-57566550-93/facebook-by-the-numbers-1.06-billion-monthly-active-users/ (Letöltés: 2013. május 9.)

European Comission (2012): Protection of personal data. European Comission, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (Letöltés dátuma: 2013. május 20.)

Kassner, M. (2012): Are you checking privacy policies frequently? TechRepublic, http://www.techrepublic.com/blog/security/are-you-checking-privacy-policies-frequently/8078?tag=content;siu-container (Letöltés: 2012. jún. 14.)

Matthew, S.J. (2012): Twitter Adds Do Not Track Capability. Information Week Security, http://www.informationweek.com/security/privacy/twitter-adds-do-not-track-capability/240000630 (Letöltés dátuma: 2012. szeptember 25.)

Murphy, K. (2010): The New York Times, http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=0 (Letöltés dátuma: 2013. március 15.)

Ohm, P. (2012): Branding Privacy. Minnesota Law Review, 97.(3): p. 907–989.

Reardon, S. (2012): FBI launches $1 billion face recognition project. New Scientist, http://www.newscientist.com/article/mg21528804.200-fbi-launches-1-billion-face-recognition-project.html (Letöltés: 2013. február 14.)

Simon Judit et al. (2011): A marketingkutatás alapjai. Budapest: Aula Kiadó

Slovak, P. (2012): How to Use Foursquare to Host a Contest. Marden-Kane, http://www.mardenkane.com/contest-best-practices/how-to-use-foursquare-to-host-a-contest.html (Letöltés dátuma: 2013. május 1.)

Szommer K. (2013): Webes adatbányászat. Matematikát, Fizikát és Informatikát Oktatók XXXVI. Konferenciája. 3., old.: 137–142. Gyöngyös: Károly Róbert Kutató-Oktató Közhasznú Non-profit Kft.

Tonder, W.v. (2011): Partentscorner. http://www.parentscorner.org.za/blog/geotagging-your-child-safe-0 (Letöltés dátuma: 2013. márc. 31.)

TsuruZoh, T. (1999): Description of Exif file format. MIT Media Lab, http://www.media.mit.edu/pia/Research/deepview/exif.html (Letöltés dátuma: 2012. március 17.)

Túri É. (2011): Digitális lábnyom keletkezése és kezelése. Bp.

Windhager-Pokol E. (2013): Bűnüldözés adatbányászati eszközökkel. Marketingkutató, http://marketingkutato.hu/bunuldozes-adatbanyaszati-eszkozokkel/ (Letöltés dátuma: 2013. nov. 10.)