JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Cookie és spyware -
az elektronikus marketing két eszköze jogi szempontból

Vikman László (vikman.laszlo@jogiforum.hu)

(Megjelent: Magyarország Médiakönyve 2003., Enamiké, 718-724. o.)

Cookie

Bevezetés

A tavalyi évben az internetes marketing máig legvitatottabb eszközével, a spammel foglalkoztam. A kéretlen elektronikus reklámüzenet után ezúttal két másik „módszert", alkalmazást fogok bemutatni, amelyek szintén veszélyeztethetik a felhasználók személyiségi jogait, illetve okozhatnak károkat a gyanútlanoknak. Az első vizsgált „jelenség", a cookie, magyarítva, süti, vagy bitsüti. Ez lényegében egy 4 kilobájtnál nem nagyobb szövegfájl, amit az internetes böngészőprogram tárol el a számítógépünkön a meglátogatott szerverekről. Funkciója, hogy kényelmesebbé tegye számunkra a szörfölést, mivel segítségével eltárolhatjuk az utolsó látogatás pontos helyét, jelszavakat, amelyekkel például zártkörű webhelyekre léphetünk be, különböző személyes adatainkat a lakhelytől a bankszámlaszámig, amivel az online vásárlás lesz lényegesen gyorsabb. Segítségével egyes megfelelően szerkesztett weboldalak testre szabhatók, sőt arra is használható, hogy barangolásunk történetét ismerve az oldalon azok a reklámcsíkok jelenjenek meg, melyek nagyobb valószínűséggel érdekelnek majd minket (targetálás – célzott kampányok folytatása).

Elméletileg tehát egy olyan megoldásról van szó, ami időt spórol meg nekünk azáltal, hogy a gyakrabban használt információkat gyorsan elérhetővé teszi, sőt nekünk magunknak elég egyetlen egyszer ezeket megadni, attól kezdve amikor a szerver elhelyezte a gépünkön ezt a bejegyzést, már az egész folyamat automatikus. Könnyen belátható, hogy éppen ezek a hasznos tulajdonságai teszik a cookie-t személyes adatainkra és privátszféránkra veszélyessé, ha alkalmazójának szándékai túlmutatnak a szörfölők kényelmének biztosításán. Nem csoda, hogy a módszert egy online-marketinggel foglalkozó cég, a DoubleClick fejlesztette ki. Azonban ne higgyük, hogy ismét csak a pénzre éhes kereskedők élnek (vissza) a cookie nyújtotta lehetőségekkel, bizony sok kormányzati honlap nézegetése közben is történhetnek olyan műveletek, amelyek végrehajtásába nem biztos, hogy beleegyeznénk.

Még veszélyesebbé válhat a technológia, ha egy ún. kirdetéskiszolgáló adserveren (mely reklámcsíkokat – bannereket – menedzsel, cookiekkal összekötve) keresztül nemzetközi szinten is kapcsolatba kerül az internetezők többségével, ez esetben idővel a csábítás nagy lehet, és a DoubleClicket is csak a közfelháborodás (no meg az esetleges presztízs- és annak nyomán az üzleti veszteség) tartotta vissza a internetezőkről szerzett tudásának értékesítésétől.

A cookie története

A cookie sem friss jelenség már, hazánkban a szaklapok úgy 4 éve írtak róla először, de inkább még csak mint érdekesség szerepelt mindenhol, az első a jog szempontjából is érdekes hírek ezúttal is a legnagyobb IT-piaccal rendelkező USA-ból érkeztek. 2000. közepén folytak tárgyalások a Federal Trade Comission és a legnagyobb online reklámcégek között. Az egyeztetés célja olyan ipari kódex kialakítása volt, mely az internetezőkről készülő adatbankokat (melyek pl. cookie segítségével készültek) szabályozná. Az FTC szerint még nem sikerült olyan kereteket kidolgozni, melyek szükségtelenné tennék az állami beavatkozást. A tét a weboldalak látogatóiról már régóta folyamatosan gyűjtött adatok sorsa volt, melyeket személyre szabott reklámok kialakítására használtak fel. Az elképzelések szerint az FTC illetékes bizottsága felügyelné, hogy a kezdeményezéshez csatlakozó cégek betartják-e a megállapodást és a meg nem engedett profilokat készítő cégeket pedig pénzbüntetéssel sújtanák. A probléma súlyára jellemző, hogy az FTC munkatársai 15 perc böngészés alatt 124 cookie-t kaptak gépükre. A marketingesek hangoztatták, hogy olyan technikát dolgoztak ki, mely anonim információkezelést tesz lehetővé, azonban a privacy-t védők szerint meg kell adni a lehetőséget arra, hogy a felhasználók megismerhessék milyen adataikat regisztrálják, és azokat kérésükre törölni kelljen ,valamint minden bizonnyal csakis az állami szabályozás jelenthet megoldást.

A bevezetőben már utaltam rá, hogy a cookie-t nem csak az üzleti szféra használja kíváncsiskodásra. Szintén 2000. nyarán keltett felháborodást, hogy a Clinton-kormányzat elgondolása szerint, a droglapokat látogató szörfölőket cookie-k segítségével követik, és megállapítják személyazonosságukat. Marc Rotenberg, az Electronic Privacy Information Center (EPIC) igazgatója szerint ez a gyakorlat megsérti mind a Fehér Ház eddigi személyiségi jogi politikáját, mind az 1974-es vonatkozó személyiségi jogokat rögzítő törvényeket.

Az amerikai kormányzat belátta tévedését, azonban ennek októberre még nem sok hatása volt. A tiltás ellenére 13 kormányhatóság használt cookie-t, sőt legalább egy esetben a szerzett információt kereskedelmi cégeknek is eladták. A hatóságok között volt többek között a

szövetségi repülésügyi igazgatóság és az egészségbiztosítási pénztár is. Az eset akkor nagy vihart kavart a szenátusban, ahol a személyiségi jogok megsértését kérték számon a hatóságok vezetőitől. Figyelemre méltó, hogy akkoriban demokrata vezetés volt, mely általában érzékenyebb a személyiségi jogokra, igaz ugyan, hogy még szeptember 11. előtt történt mindez.

Az EU is 2000 nyarán kezdett el foglalkozni az Internettel kapcsolatos adatvédelmi problémákkal, a cookie a spammel együtt került terítékre. A már ott is említett és később elfogadott irányelv első tervezete szerint a felhasználóknak csak akkor lehet majd cookie-kat küldeni, ha ők előzőleg beleegyeztek - ami történhet kattintással is.

2002. tavaszára a Progress & Freedom Foundation megbízásából elemzés készült arról, hogy a kereskedelmi website-ok üzemeltetői milyen mértékben gyűjtenek személyes információkat felhasználóikról. A kutatómunka során az Egyesült Államok 100 legnagyobb elektronikus kereskedelmi vállalkozását és 300 kisebb, véletlenszerűen választott honlapot vizsgáltak. A 2001 decemberében végzett felmérési adatok szerint a cégek jóval kisebb mértékben gyűjtenek be adatokat ügyfeleikről, illetve honlapjuk látogatóiról. Csökkent mind az e-mailen keresztül lefolytatott adatgyűjtés, mind pedig a harmadik féltől érkező cookie-k terén. Utóbbi arra a korábban több botrányt okozó gyakorlatra utal, mely során a felhasználó által meglátogatott weboldal gazdái a látogató azonosítására szolgáló saját eszközön kívül (cookie), mások - például egy hirdető partner - számára is lehetővé teszik ugyanezt. Ezt először a cookie-t megalkotó DoubleClick tette meg, ezzel jókora port kavarva. A szakértők szerint a változás az internetes kereskedelmi piac konszolidálódásának a jele, a siker érdekében korábban számos eszközt bevető cégek ma már nem csak elhelyezik honlapjukon az adatvédelmi irányelveket, de be is tartják azokat. Egy, az Ernst & Young megbízásából készített elemzés szerzői pedig jelentős lépésként könyveli el a P3P-technológia terjedését. A Platform for Privacy Preferences projekt által kidolgozott technológiával az eljárást alkalmazó honlapok látogatói saját maguk is megbizonyosodhatnak személyes információik státuszáról.

Mikor az EU új adatvédelmi irányelve tavaly tavasszal kezdett „beérni", egyre többet lehetett hallani a spam-ről, cookie-król. Az angolok és az opt-in spam szabályozást támogatók közötti alku és eredménye ismert, a cookie körül is volt bőven vita. Április közepén úgy tűnt, az eszköz betiltásra kerül, ez ellen azonban az üzleti élet szereplői hangosan tiltakoztak. Véleményük szerint ez elriaszthatja ügyfeleiket, és hátrányos helyzetbe is hozhatja őket a világ más részein működő cégekkel szemben, amelyek liberálisabb szabályok közt működhetnek. Az Európai Parlament emberi jogi bizottsága ekkor még a sütiket, a kémszoftvereket, valamint a bugokat (lásd lent),

amelyek szintén veszélyeztetik az internetes biztonságot, mind egy kalap alá vette, azt állítva róluk, hogy súlyosan megsértik a felhasználónak a titokhoz való jogát. A munkaadókat tömörítő európai szövetség (UNICE) azonban azt ajánlotta fel, hogy a felhasználót a gép automatikusan tájékoztassa arról, hogy adatait feldolgozzák, és tegyék lehetővé számára lehetővé ennek korlátozását. A legnagyobb internetes könyv- és CD-kereskedő cég, az Amazon.com egyenesen rémálomnak nevezte a parlament döntését, mivel ez alapjában forgatná fel eddigi rendszerüket és jóval kényelmetlenebbé tenné az elektronikus kereskedelmet, melynek ösztönzése pedig fontos prioritás.

Április végére engedékenyebb lett a parlament, olyannyira, hogy nemcsak hogy nem tiltják, de a felmerült felhasználói előzetes engedélyt sem kötötték ki, csak azt, hogy a felhasználó hozzáférhessen a PC-jére „aggatott" sütik tartalmához. Ezt az eredményt nagyrészt az internetes vállalatokat és online reklámokkal foglalkozó cégeket tömörítő Interactive Advertising Bureaunak sikerült elérnie. „Felsoroltunk több, mint egy tucat olyan következményt, amellyel ez a döntés járna az online kereskedelemben és reklámiparban. Sőt az is látható, hogy a cookie-használat ilyen mértékű szigorításával megtizedelődne az online piacon működő vállalatok száma." mondta az IAB elnöke, Danny Meadows-Klue. A véglegesen kibocsátott irányelv később azonban mégsem ezt tükrözte, hanem az adatvédők követeléseinek megfelelő előzetes engedélyezési eljárás került a direktívába, mely alapján a tagállamok kialakítják majd saját szabályozásukat.

A süti fejlődése

Az egyszerű 4 kilobájtos szövegfájl tulajdonságai, de főleg az alapjául szolgáló ötlet sokak fantáziáját megragadta. Tulajdonképpen évente jelentek meg új, az eredeti elgondoláson alapuló, de továbbfejlesztett megoldások. Az első 2000-ben került napvilágra. A Microsoft által fejlesztett Internet Explorer egyik beépített eleméről, a Persistence-ről van szó. Ennek segítségével a webszerverek képesek a felhasználó számítógépén személyes adatokat tárolni, mint például keresési adatokat és beállításokat, lényegében olyan mint az ős, ugyanúgy lehetetlenné teszi az inkognitó megőrzését, de lényeges különbség, hogy a felhasználó által nem kontrollálható, pontosabban a kiiktatásának ára a scripting funkció kikapcsolása, ami viszont megakadályozhatja a webes menükezelést és az email-küldést. A Persistence az IE 5.0-s verziótól van jelen, és miután lelepleződött 2000. októberben a Microsoft ígérete szerint fontolóra vették, hogy eltávolítják a programból.

2001 újdonsága a „bug", ami ezúttal nem programhibát, hanem poloskát jelent. Ez egy kis képpont a HTML-kódban (a weboldalakat kinézetét meghatározó számítógépes nyelv), amelyek cookie-khoz is kapcsolódhatnak, és biztonsági szakértők szerint elvileg akár ártó szándékú programokat is elhelyezhetnek a felhasználó gépén (lásd spyware). Richard Smith, a Privacy Foundation egyik vezetője nyilatkozata szerint „minden web bug-ot használó cégnek világosan jeleznie kellene ezt a privacy policy-jében azzal együtt, hogy milyen célból teszi ezt; hogy milyen adatokat gyűjtenek be így, hogy kikhez jutnak el az adatok; és azok, akikhez eljutnak az adatok, mire használják fel ezeket". Az alapítvány épp az ilyen jellegű visszaélések ellen küzd, többek közt programok (pl.: böngésző plug-inek) fejlesztésével is, melyek kiszűrik az ilyen támadásokat.

A tavalyi évben jelent meg a biscuit, mely nevében is rokon az előddel. A Strathclyde University-n kidolgozott rendszer a projektet vezető Dr. Lykourgos Petropoulakis szerint - a cookie-val ellentétben - majdnem bármilyen információt képes begyűjteni, miközben gyakorlatilag lehetetlen észrevenni. A passzív szövegfájl helyett olyan szenzorprogramot alkalmaznak, ami nem csak a billentyűleütéseket képes rögzíteni, de minden más felhasználói tevékenységet is nyomon követ az interneten (egy adott cookie csupán egy adott site-tal kapcsolatban működik!). Emellett távolról meg lehet változtatni, hogy jobban igazodjon a felhasználó vagy a tulajdonos igényeihez. A potenciális felhasználók között vannak többek között az online kereskedők, az alkalmazottaikat megfigyelni akaró munkáltatók és a biztonságtechnikai cégek (akik meg akarják gátolni, hogy a felhasználók nem megfelelően használják a szoftvereket). Alkalmas lesz a meghatározott tartalmú site-okhoz, dokumentumokhoz, adatokhoz, e-mail-ekhez való hozzáférés meggátolására is. Ha pedig egy vállalkozás kereskedelmi adatokat akar majd gyűjteni, úgy - a mostani elképzelések szerint - a felhasználó a letöltésért cserébe pénzt vagy kedvezményeket kaphat. De - mutat rá a hírt közlő The USA Register - amennyiben „teljesen világos, hogy a felhasználót figyelmeztetik, mielőtt ilyen (biscuit) települne a gépére, akkor felesleges lenne azt hangsúlyozni, hogy nehéz észrevenni és megsemmisíteni". Valóban komoly kérdés az, hogy mit kezdenének az online szereplők egy ilyen „szupersütivel". Minden bizonnyal egy ésszerű és a személyiségi jogokat tiszteletben tartó best practice kialakulásáig sokak értékes és érzékeny adatai kerülnének illetéktelen kezekbe. Olyan mértékű ellenőrzést tenne lehetővé az alapvetően szabad légkörű Interneten ami alapjaiban változtatná meg a háló világát és biztos, hogy nem a jó és kívánatos irányba.

Spyware

Bevezetés

A spyware (adatokat gyűjt), vagy ad-ware (reklámokat „szolgáltat") kategóriába akkor kerül be egy egyébként látszólag teljesen hétköznapi szoftver, ha vannak bizonyos rejtett funkciói, melyek a program futtatójának tudta és/vagy akarata nélkül telepítődnek, és gyűjtenek össze információkat a számítógép felhasználójáról, amelyeket vagy visszaküldenek az alkotónak, vagy amelyek alapján többé-kevésbé személyre szabott hirdetésekkel bombázzák a felhasználót. A legtöbbször ezek a programok ingyenesen hozzáférhetők, vagy kereskedelmi programok shareware, vagy lite verziói. Általában böngészők, fájlmegosztó alkalmazások, letöltés-vezérlők, médialejátszók és online játékok rejtenek ilyen nem kívánatos kódrészleteket. Akkor buknak le rendszerint, amikor egy gondos számítógép-tulajdonos által feltelepített tűzfalban fennakad az üzenet, amit a készítő szerverének próbál meg elküldeni a sanda kis program. A „kéretlen programok" létét olykor feltüntetik a szoftverrel járó felhasználói szerződésben vagy egy külön readme-fájlban, de szerencsére ma már arra is van példa, hogy installálás közben opcionálisan ki lehet kapcsolni őket. Ám a legtöbb felhasználó kapkodva és nem kellő odafigyeléssel szokott telepíteni, ezzel a figyelmetlenséggel a kémszoftver készítőjének malmára hajtva a vizet.

A spyware története

Az első hírek az ilyen jellegű alkalmazásokról 2000. közepe táján jelentek meg. Akkor írt a Wired című online magazin arról, hogy az America Online (AOL) komoly per elé néz, mint a Netscape böngésző tulajdonos-fejlesztője, ugyanis a szoftverben megvalósított, egyébként műszakilag kiváló, SmartDownload technológiáról kiderítették, hogy az alkalmas a személyiségi jogok megsértésére. Egy New Jersey államban működő cég weboperátorának tűnt ez fel, miután a cég azonnal beperelte az AOL/Netscape párost. A cég szerint, a letöltőhelyek cégei a böngésző segítségével rögzítik az internet szerverek és a felhasználók közötti forgalmat. A Netscape Communicator SmartDownload funkciója pedig titokban megküldi a letöltés adatait az AOL tulajdonú Netscape-nek.

Ez két 1986-os törvény (Electronic Communications Privacy Act of 1986, Computer Fraud and Abuse Act of 1986) megsértését jelentette a felperes álláspontja szerint, amelyeket a digitális adatok védelmére hoztak. A Netscape Communicator dokumentációja a SmartDownloadról csak annyit említett, hogy az segíti a letöltések intelligens lebonyolítást, beleértve például a

félbeszakítást és folytatást. A letöltés közben pedig „informatív jelleggel” mutatja a Netscape Netcenter lapját. Nos, a gyakorlatban nem csak ezért vette fel a kapcsolatot a Netcenterrel. Pedig a Privacy Policy-ben a Netscape azt ígérte, hogy a profilinformációt csak a letöltött állományhoz csatlakozó hasznos más információk megkeresésére, és a letöltő jobb tájékoztatására használják, különben nem rögzítik, továbbá ez a lehetőség kikapcsolható. Az eset egyértelműen precedens súlyú volt, várható volt hát, hogy cégek sorát fogják hamarosan tiltott elektronikus adatgyűjtéssel vádolni.

2001. májusában lehetett ismét sokat hallani a spyware-kről, ezúttal a Napster típusú peer-to-peer fájlmegosztó rendszer egyes klónjaival kapcsolatban. Számos ilyen – elsősorban mp3 formátumú zeneszámok és videofájlok letöltésére használt - program olyan szoftvert is telepített, mely reklámokkal árasztotta el a felhasználót, vagy nyomon követte internetes tevékenységét. Többek között a Bearshare, az Audio Galaxy Satellite és az iMesh is így próbált pénzre szert tenni cserébe az "ingyen-szoftverért", ezzel közben súlyosan sértve a felhasználók privacy-jét. A fájl-megosztó rendszerek gyártói, így Vinnie Falco, a BearShare Gnutellá-t gyártó FreePeers egyik technikai vezetője is arra hivatkozott, hogy „valahogyan az ingyenes szoftverből is pénzt kell csinálni”, ha továbbra is ingyen akarják adni, és a mostani helyzet „a felhasználók privacy-jének védelme, valamint az ingyen szoftver biztosítása közötti kompromisszum”. (Idén nyárra viszont már a Morpheus és a Kazaa fájlcserélők új verziója is védi a felhasználók privacy-jét, tehát spywarementes és biztosítja a teljes anonimitást.)

Ilyen megoldásokkal természetesen nem csupán a kis cégek kísérleteztek: a RealNetworks (a népszerű RealPlayer és más multimédiás alkalmazások gyártója) is spyware-t csatolt néhány termékéhez. Az akkori adatok szerint az Audio Galaxy programját 6,8 millióan töltötték le a download.com-ról, a Bearshare-t pedig több mint 3 millióan. Az Audio Galaxy-val együtt utazó Offer Companion pedig nem csak hirdetéseket jelenít meg, de különféle adatokat (pl. felhasználói szokások, e-mail címek) is visszaküld a szoftvert gyártó Gator.com-nak. Egy ekkortájt összeállított lista több mint 800 olyan programot sorolt fel, melyben spy- vagy adware található.

A következő hónapban már egy hardver-gyártó is, név szerint a hangkártyákat gyártó Creative Labs is gyanúba keveredett, ugyanis a gyártó termékeinek drivereivel az Interneten keresztül kommunikáló szoftver is települt. A cég szerint ez a newsupd.exe nem kémprogram, hanem a felhasználók automatikus frissítését segítő szolgáltatás. Ennek némileg ellentmondott, hogy a szoftver a Creative legtöbb programjával együtt települ, és a felhasználók engedélye (sőt, tudta)

nélkül létesít kapcsolatot a cég weblapjával. Emellett olyan opciója sem volt, mely lehetővé tette volna a kikapcsolását a telepítés során.

A Creative európai márkamenedzsere, Franco Debonis azt állította, hogy a kérdéses program „semmit nem csinál, ha nem vagy felcsatlakozva az Internetre, rendszeresen ellenőrzi viszont, hogy él-e a kapcsolat, és ha igen, akkor megnézi, hogy nem jelent-e meg a szoftver frissítése". Egy könnyen megtalálható kikapcsolási opció pedig azért hiányzott eddig, mert a fejlesztők egyszerűen nem gondoltak rá, hogy igény lenne ilyesmire, de a következő verziókba már beleépítik és fel is fogják erre a szolgáltatásra hívni a figyelmet. Ugyanakkor ez ellen szól, hogy a newsupd.exe különböző információkat is küldött a cég szervereinek - de Debonis szerint semmi személyhez köthetőt: legfeljebb olyasmit, hogy „erre a bannerre ráklikkeltek".

Tavaly januárban ismét fájlcserélő-szoftverek kerültek a figyelem középpontjába. A többek között antivírus-szoftvereket készítő Symantec jelentése szerint a népszerű Grokster és Limewire szoftverek spyware programokat tartalmaztak. A rejtett kód nem okozott kárt a számítógépekben, de bizalmas adatokat küldött el meghatározott weboldalaknak, mint pl. a felhasználó azonosítója és internetcíme. A „Clicktilluwin", egy online lottó kliensszoftver, mely egyben reklámokat is megjelenített, a fájlcsere-alkalmazásokkal együtt került fel a felhasználó számítógépére, és egy „W32.DlDer" programot is csatol, amelyet a Symantec trójai falóként azonosított. A trójai falovak, mint ismeretes, részben (vagy teljesen) átveszik a számítógép irányítását, hogy saját utasításaikat végrehajtsák. A Symantec bejelentését követően egyébként számos felhasználó a FastTrack KaZaA programja esetében is hasonló problémába ütközött.

A Limewire szóvivője röviddel ezután elmondta, hogy a társaság a kiadta szoftverének új verzióját, amely már nem tartalmazza a trójai falovat rejtő Clicktilluwin-t. Greg Bildson, a Limewire technikai igazgatója elmondása szerint a társaságnak nem volt tudomása a kémprogramról. A Grokster készítői elnézést kértek a felhasználóktól, és kiadtak egy programot, amely eltávolítja a spyware kódot a számítógépről. „Nincs hozzáférésünk a reklámszoftverek forráskódjához, ezért csak arra támaszkodhattunk, amit a reklámozók állítottak a programról" - állt a társaság weboldalán.

Tavaly nyáron a sorozatos visszaélések miatt Az Európai Unió számos egyéb szoftver mellett a zene-, illetve médialejátszókat is nagyító alá vette. A szabályzóbizottság szakértői elsősorban azt kezdték vizsgálni, miként kezelik a szoftverek a felhasználók személyes adatait. A legáltalánosabb ilyen típusú szoftvereket a Microsoft és RealNetworks cégek készítik és mindkettő esetében volt

ok a vizsgálatra. A RealNetworks épp ezidőtájt újította meg szerződését a Gracenote-tal, amely társaság szoftvere információt nyújt a felhasználónak az általa hallgatott zene CD-ről. A társaság által kezelt információk pedig a felhasználó tudta nélkül, könnyedén összegyűjthetők marketing célokra. A RealNetworks szóvivőnője szerint a társaságot az EU még nem kereste meg az ügyben, és a kérdéses szoftver egyébként sem köti az információkat az egyes felhasználókhoz. „Teljesen nyíltak vagyunk adatvédelmi irányelveinket illetően" - mondta Erika Shaffer, aki hozzátette, hogy a felhasználók letilthatják a Gracenote szolgáltatásának használatát, és együttműködést ígért az esetleges felülvizsgálat esetén. A Microsoft esetében szintén merültek fel aggályok mégpedig a Passport szolgáltatással, és a Windows MediaPlayer egy rejtett funkciójával kapcsolatban, amikor a szoftver értesíti a Microsoftot arról , hogy a számítógépen milyen állományokat játszottak le.

Az összefoglalót a Netscape-féle SmartDownload szoftverrel kezdtük. Ez az ügy 2002. októberében zárult le jogerős ítélettel a Szövetségi Fellebbviteli Bíróság előtt. Az ítélet szerint a Netscape a böngésző felhasználói licencszerződése alapján sem volt jogosult titkos információk gyűjtésére a felhasználókról, valamint a kémkedési opció miatt is elmarasztalták az alperest. A fellebbviteli bíróság elsősorban azért ítélt a felperesek javára, mert a külön licencszerződést a megszokott eljárási móddal szemben nem kellett végigolvasniuk és elfogadniuk a felhasználóknak a telepítés sikeres végrehajtásához. Az ítélet így megnyitotta a kaput a hasonló perek felé, melyekben a hasonló szoftverek készítői ellen léphetnek fel a felhasználók. Azonban a döntés alapja is felhívta a figyelmet arra, hogy tanácsos legalább pár pillantást vetni a telepíteni kívánt szoftver licenszére, ezzel sok kellemetlenség spórolható meg később.

Tavaly novemberi hír volt, hogy a Gator online marketing céget már hét nagy szervezet perelte be, mivel meglehetősen vitatható módon automatikusan megnyíló hirdetési ablakokat (pop-up ads) helyez el webhelyeiket, és ezzel megtéveszti a webhelyre látogatókat. A Six Continents Hotels és az Inter-Continental Hotels is hasonló értelmű keresetet adott be a Gator ellen, mert a cég agresszív hirdetéseivel egyrészt megsérti a szállodák márkanevükhöz fűződő jogát, másrészt megtéveszti a szálloda ügyfeleit. A problémát az okozza, hogy a hirdetési ablakokról azt hiheti az ügyfél, hogy a szállodalánchoz tartoznak, és ott bonyolítanak le helyfoglalást, majd amikor megérkeznek úti céljukhoz, kiderül, hogy a szállodalánchoz tartozó hotelben nincs a nevükre lefoglalt szoba. A felperesek a Gator „OfferCompanion" kémszoftverének működését nehezményezték elsősorban. A program más szoftver letöltése közben - mintegy trójai falóként - letöltődik a felhasználó PC-jére, és automatikusan futni kezd, amint a felhasználó megnyitja a

böngészőt - és a különböző webhelyekre látogató felhasználót a hirdetési ablakokkal igyekszik onnan átcsábítani a Gator ügyfeleinek webhelyeire.

Látható hát, hogy ez az egyébként nagyon elmés módszer sem az EU-ban, sem az Egyesült Államokban nem talált kedvező fogadtatásra, sem a felhasználók, sem a hatóságok részéről. Ennek utóbbiak már jogerős és precedensértékű ítéletekkel, valamint sorozatos vizsgálatokkal adtak hangot. A már többször említett tudatosság megjelenése a szoftverek üzemeltetésével kapcsolatban pedig tovább csökkentheti azokat a gyenge pontokat ahol a direktmarketing szakmának azon része - mely a számára fontos információk megszerzésekor agresszív és a legalitásra aránylag kevésbé kényes - hozzáférhet személyes vagy érzékeny adatainkhoz.

Első Magyar Jogi Portál
és online Ügyvédi Szaknévsor

JOGI FÓRUM

jogi hírek

interjúk

publikációk

vitafórum

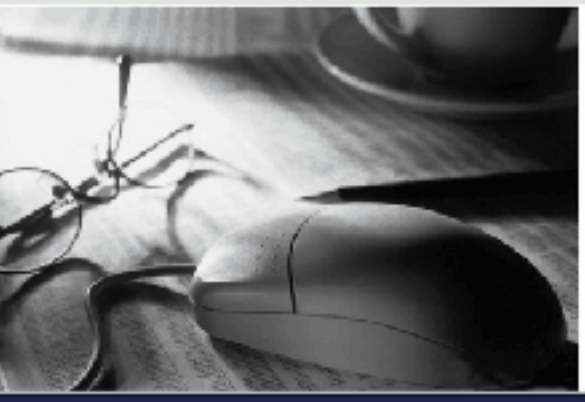
szaknévsor

jogi szakkönyv-katalógus

jogi állásbörze

szakmai rendezvények

heti hírlevél



országos ügyvédi szaknévsor

magyar, angol és német nyelven

ügyfél keres ügyvédet szolgáltatás

www.jogiforum.hu