poročilo

POLETNA ŠOLA *IFIP 2010*

Šesto mednarodno poletno šolo (IFIP Summer School[1]) so organizirali v sklopu EU projekta PrimeLife[2] v sodelovanju z IFIP (International Federation for Information Processing). Potekala je v Helsingborgu na Švedskem od 2. do 6. avgusta 2010, pod naslovom *Privacy and Identity Management for Life,* osrednja tema pa je bila upravljanje z zasebnostjo in identiteto v prihajajočih spletnih aplikacijah skozi vse človeško življenje (*Privacy and Identity Management for Emerging Internet Applications throughout a Person's Lifetime)*. Zvrstilo se je večje število predavanj, dve panelni razpravi in več paralelnih delavnic, na katerih so svoje prispevke predstavljali študenti. Za razliko od delavnic, ki so potekale v hotelu Clarion Grand, so dopoldanska predavanja potekala v najstarejši ohranjeni hiši v Helsingborgu, in sicer v Jakob Hansens Hus.[3]

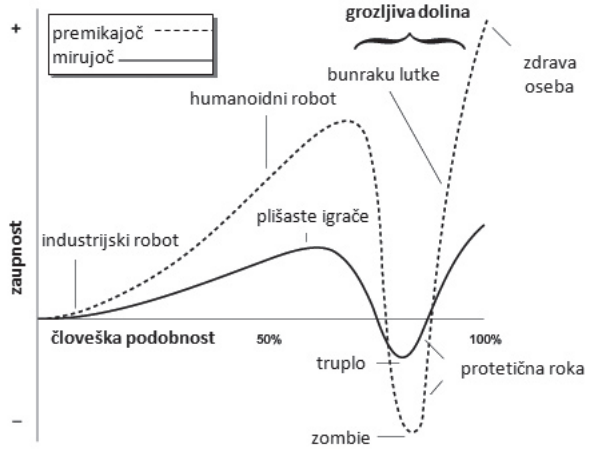
Bibi van den Berg (Tilburg University) je predstavila zanimiv pogled na tehnologijo in zasebnost *(The uncanny valley everywhere: On autonomic technologies and privacy)*. Socialne mreže in druge spletne aplikacije različnih ponudnikov je primerjala z robotiko, pri čemer se je oprla na članek *Masahira Morija, The Uncanny Valley.*[4]

Povod za takšno razmišljanje sta bila dva neljuba dogodka. Pri prvem se je neki osebi med e-pošto pojavilo vabilo v socialno mrežo Facebook, katere član oseba ni bila. V pošti je bil seznam ljudi, ki naj bi jih ta oseba poznala in zastrašujoče je bilo, da jih je res vse poznala. Drugi primer temelji na izkušnji z Google Buzzom, ki ponuja posodobitev podatkov o naših prijateljih in možnost, da jim sledimo. Uporabniki so se obojega ustrašili, saj niso vedeli, od kod so spletni ponudniki storitev dobili vse te informacije, in so to dojemali kakor vdor v svojo zasebnost.

V robotiki poznamo tri linije razvoja:

1. Mehanični roboti (angl. *mechanoid robots*) so predvsem industrijski roboti, katerih prvotna naloga je funkcionalnost (robotske roke).
2. Humanoidni roboti (angl. *humanoid robots*) so roboti, po konstrukciji že podobni ljudem (ASIMO, AIBO).
3. Androidni roboti (angl. *android robots*) so roboti, ki želijo biti v vsem, kolikor je le možno, podobni ljudem (Saya, Kansei).

Mori deli robote v štiri skupine, glede na to, kako jih ljudje sprejemamo (slika 1). Roboti, ki so ljudem že zelo podobni, vendar se ne obnašajo kot ljudje, so za večino zastrašujoči. Sodijo v tako imenovano skrivnostno, grozljivo dolino (angl. *uncanny valley*). Mori nas svari pred razvojem in izdelovanjem tako imenovanih androidov, ker jih je težko narediti popolne oziroma takšne, da se jih ljudje ne bi bali. Tako imenovane zdrave osebe (angl. *healthy persons*) so roboti, ki bi zelo dobro posnemali ljudi in bi se mi ob njih dobro počutili.



Slika 1: Prikaz, kako ljudje sprejemajo različne robote

Bibi van den Berg je poskušala ta način razmišljanja prenesti na programje in spletne aplikacije. Podobnosti in povezave je prikazala takole:

	videz	⟶	**vedenje**
Mori – robotika	zapleteno	grozljiva dolina	enostavno
Berg – programje	enostavno		zapleteno

Podobno kot Mori za robote pravi Bibi van den Berg za programsko opremo, da se čudno počutimo, kadar se srečamo z nekim servisom, ki je na pogled enostaven, vede pa se zapleteno. Facebook in Google Buzz se nahajata v tej grozljivi dolini, saj sta na pogled in za

uporabo zelo preprosta, ko pa enkrat delujeta, dobimo kopico podatkov, kar je zastrašujoče. Predstavila je nekaj zamisli, kako ob upoštevanju človeške narave izboljšati socialne mreže:

- ob podatkih, ki nam jih neki servis ponudi (npr. Facebook), navesti način, kako so bili podatki pridobljeni;
- ob seznamu ljudi, ki naj bi jih poznali, imeti možnost izbrati, ali nas to zanima ali ne.

Google je z Google Buzzom želel ponuditi obliko pomoči uporabnikom, lahko pa smo videli, koliko podatkov imajo in kaj zmorejo. Tega se je veliko uporabnikov prestrašilo, saj se večina ne zaveda, kaj Google počne in česa je zmožen. V navedenih primerih se v več pogledih krši zasebnost, in sicer gre za nadzor, povezovanje podatkov o nas z različnih področij ipd.

Vprašanje je, ali lahko prestopimo grozljivo dolino na področju socialnih mrež. Za dosego cilja bo treba v delovanje socialnih mrež vključiti dejavnike iz realnega sveta, ki so v uporabi že stoletja. Tako bi na primer le prijatelji lahko predlagali nove znance in to ne bi potekalo avtomatizirano.

Za konec je predstavila še splošen pogled na nove tehnologije, ki bodo uporabljale poosebljanje in bodo proaktivne. Te nove tehnologije bodo vedele, kje se nahajamo ali s kom komuniciramo, in bodo prilagojene posamezniku; npr. človeku na avtobusni postaji bo predlagano, naj se lahko pelje z naslednjim avtobusom, ker bo ta aplikacija razpolagala z informacijo, da gre ta človek danes ob določeni uri na neki sestanek na določen kraj.

Alma Whitten (Google[5]) je predstavila načine, kako Google varuje osebne podatke svojih uporabnikov *(Privacy Research at Google)*. Google je najbolj znan po istoimenskem spletnem iskalniku, ki je na voljo uporabnikom interneta po vsem svetu, ponujajo pa še več drugih priljubljenih aplikacij, kot so YouTube, Gmail, Google Earth idr.

Pri Googlu na vseh nivojih razvoja razmišljajo o varovanju zasebnosti, saj je pomembna za njihove uporabnike. Če ne bodo ponudili uporabnega nadzora in dobrega varovanja podatkov, jih bodo uporabniki enostavno zapustili.

Naštela je pet vodilnih načel, ki vodijo Googlovo razmišljanje o zasebnosti:

- uporabiti zbrane podatke in na tej osnovi svojim uporabnikom ponuditi koristne storitve in proizvode,
- razvijati proizvode, ki v praksi upoštevajo visoke standarde zasebnosti,
- poskrbeti, da je zbiranje in uporaba osebnih podatkov pregledna,
- dati uporabnikom jasno in uporabno izbiro varovanja njihove zasebnosti,
- odgovorno skrbeti za zbrane in hranjene podatke.

Pri Googlu naj bi uporabili pridobljene informacije le v primerih, kadar lahko z njimi uporabnikom zagotovijo neko korist. Zavezani so preglednosti, nadzoru s strani uporabnikov in zaščiti pridobljenih podatkov. Predavateljica je zatrdila, da zbranih osebnih podatkov svojih uporabnikov ne tržijo in ne prodajajo. Pri razvoju proizvodov jih vodi želja po vključevanju zasebnosti in varnosti. Ker se Google financira predvsem s spletnim oglaševanjem, so lahko njihovi proizvodi in storitve prosto dostopne za osebno rabo. Uporabniki dobijo brezplačne storitve, oglaševanim podjetjem pa Google z inovativnim sistemom oglaševanja posreduje povratne informacije, s katerimi lahko izboljšajo svojo ponudbo. Veliko spletnih strani uporablja Googlov program AdSense za prikaz oglasov in njihov cilj je narediti te oglase čim bolj relevantne za uporabnike. Pri tem si neprestano prizadevajo ohraniti preglednost in uporabnikov nadzor nad uporabljenimi podatki v njihovem oglaševalnem sistemu. Povedala je, da njihova ekonomija temelji na "klikih" uporabnikov, to je na izbiri najustreznejše povezave iz seznama rezultatov. Pri tem se tej povezavi izboljša rang strani (angl. *page rank*), po katerem so razporejene strani v iskalniku. Torej se na neki način Google uči od svojih uporabnikov.

Podrobneje je predstavila še ciljno oglaševanje. Poudarila je trud, da ne prikazujejo neprimernih oglasov, tako da se ob novici o bombnem napadu ne prikaže neprimerna vsebina. Omenila je primer, ko je pred leti prebirala novico o podivjanem šoferju buldožerja in na strani zagledala oglase za prodajo buldožerjev. Ciljnega oglaševanja tudi ne uporabljajo v zvezi z občutljivimi temami, kot so zdravje in podobno, ali temami, ki se navezujejo na otroke, mlajše od 13 let, ali druge občutljive interesne skupine. Z uvedbo Ads Preferences Manager[6] je Google postal prvi večji spletni ponudnik, ki omogoča uporabnikom pregledovanje in urejanje lastnih interesnih skupin, ki jih uporabljajo za ciljno oglaševanje. Ads Preferences Manager omogoča uporabniku vpogled v teme, s katerimi ga Google povezuje s pomočjo piškotkov (angl. *cookie*), shranjenih na brskalniku. Omogoča tudi dodajanje interesnih skupin, ki so pomembne za posameznika, in brisanje vseh, ki mu ne ustrezajo ali ne želi biti povezan z njimi. Kot zanimivost je povedala, da so pri testiranju ugotovili, da jim uporabniki bolj zaupajo, če imajo možnost neke kontrole. Tako so le štirje od desetih uporabnikov spremenili nastavitve svojih interesnih skupin. Pri Googlu so tako prišli do zaključka,

da spletni uporabniki cenijo preglednost in nadzor ter da bolje sprejemajo zbiranje podatkov in njihovo uporabo, kadar jim možnost pridobivanja podatkov ponudijo pod njihovimi pogoji, z vpogledom in neko kontrolo.

Naslednja tema so bile težave pri vključevanju zasebnosti in varnosti v nove inovativne proizvode. Kljub prizadevanjem, da se uporabnikom ponudijo transparentnost, varnost in kontrola, se pojavita dve težavi. Prva se nanaša na zbiranje in uporabo podatkov, druga pa na izboljšanje komunikacije s posamezniki in upravljanje njihove zasebnosti.

Google od svojih uporabnikov vsak dan pridobiva različne podatke. Poskušajo jih zbirati transparentno in, kadar je le možno, dati kontrolo uporabnikom. Pridobljeni podatki so zelo pomembni za Google, saj z njihovo pomočjo izboljšujejo svoje izdelke in varujejo omrežja pred hekerji, pošiljatelji neželene pošte in goljufi. Temu se zoperstavljajo s hranjenimi dnevniki (angl. *log file*). Zatrdila je, da Google ne manipulira z zbranimi podatki, da jih ne identificira ali kakor koli zlorablja. Predstavila nam je podatke, ki jih Google zbira oziroma hrani. Podatke je razdelila v tri kategorije, kot je predstavljeno na sliki 2.

Slika 2: Prikaz pridobivanja različnih vrst podatkov

Pri Google search zbirajo: datum, URL-naslov, iskalne zahteve, IP-naslov, lokacije, jezik ... Tem podatkom nato pripišejo še izbrani rezultat, vendar vseh teh podatkov ne uporabljajo za povezovanje oseb z iskanji. Vse zbrane podatke dobro varujejo, ker se zavedajo možnosti zlorab in želijo upravičiti zaupanje svojih uporabnikov. Podatke ščitijo predvsem z anonimizacijo (vsak podatek se hrani v tako imenovanem sodu skupaj z 255.000 drugimi). Po 9 mesecih v IP-naslovu pobrišejo zadnje številke za piko, po 18 mesecih brišejo piškotke (te hranijo dlje časa, ker imajo uporabniki sami možnost brisanja).

Googlovo poslanstvo je organizirati svetovne podatke (informacije) in jih predstaviti uporabnikom na splošno dostopen način. Izpostavila je tudi, da so zelo ponosni na svoja prizadevanja, kako bolje razumeti svoje uporabnike in bolje spoznati njihov način zbiranja, hranjenja in varovanja podatkov.

Claire Vishik (Intel) je predstavila povezanost med zasebnostjo, zaupanjem in varnim okoljem *(Privacy models and building trusted environments)*. Ob vedno bolj sofisticiranih napadih in zaostajanjem varnostnih sistemov se zastavlja vprašanje, ali lahko zaupamo svojim osebnim računalnikom in drugim napravam in kako lahko zagotovimo, da bo entiteta (sistem, naprava ...) delovala na določen način za specifičen namen. Naštela je tri glavne lastnosti, ki jih mora imeti neko računalniško okolje, da mu bodo uporabniki zaupali:

- varovanje s strojno opremo, ki jo obstoječa programska oprema dobro izkorišča;
- sposobnost prepoznavanja napak in zagotavljanje zaščite ob odkritju napake;
- mehanizem za preverjanje konfiguracije podatkov, ki jih posreduje neko računalniško okolje.

Po njenem mnenju se po pomoč lahko obrnemo na zaupanja vredno računalništvo (angl. *trusted computing*) ali pa na potrdila in certifikate, ki zagotavljajo informacije o varnostnem statusu okolja.

Cilj računalništva, ki je vredno zaupanja, je ustvariti bolj zanesljive računalnike z uporabo ustrezne strojne in programske opreme, ki ji bodo uporabniki in ponudniki storitev lahko zaupali. Naprave s to tehnologijo bodo lahko varovale programsko opremo pred neželenimi spremembami in bodo preverjale pristnost računalniškega okolja. Osnova pri opisu specifikacij bi bil varni čip (angl. *trusted platform module – TPM*), običajno vgrajen v napravo. Ključne značilnosti takšnega čipa so:

- dokazuje pristnost okolja, stroja, naprave,
- shranjuje neokrnjene podatke o varnostnem statusu okolja,
- zasidra vir zaupanja za neko okolje,
- varno generira, shranjuje in upravlja s šifriranimi ključi,
- se zavaruje pred programskimi napadi,
- je v celoti pod nadzorom lastnika, kar je pomembno za področje zasebnosti.

Pri potrdilih ali certifikatih pa lahko uporabniki pred interakcijo ocenijo stopnjo zaupanja v neko računalniško okolje.

V informacijskem svetu imamo zelo kompleksno ponudbo različnih omrežij in storitev, vendar vsaka družba (Facebook, eBay, Fidelity ...) našo zasebnost razume na svoj način. Večina ponudnikov spletnih storitev nam pri uporabi njihovih strani namesti razne sledilne programčke (piškotke), s katerimi pridobijo podatke o nas. Zato izkušnje uporabnikov z zasebnostjo na spletu niso vedno pozitivne.

Naštela je nekaj primerov uporabe omrežij in storitev, pri katerih je potrebno naše zaupanje:

- dostop do kritičnih sistemov,
- socialne mreže,
- spletno bančništvo in poslovanje,
- uporaba bankomatov,
- uporaba zdravstvenih storitev,
- posodabljanje in sinhronizacija raznih naprav z osebnim računalnikom.

Elektronsko poslovanje je prisotno v vseh razvitih državah in postaja rutinsko opravilo za vedno več ljudi. Očitno je dovolj zaupanja v digitalno gospodarstvo, da je elektronsko poslovanje še vedno v porastu.

Naštela je še nekaj običajnih groženj, ki ogrožajo varnost in zasebnost danes:

- informacije o kreditnih karticah,
- zaupni podatki o bančnih računih,
- dostop do e-pošte.

Navedla je zanimiv primer, ko nam pri registraciji na neko spletno mesto najprej pošljejo kriptografirano stran za prijavo, nato pa nam vrnejo sporočilo, ki vsebuje geslo kar v besedilu, in primer telefonskih donacij, ki naj bi bile anonimne, vendar nas operater na začetku identificira. Različne tehnologije moramo začeti gledati in jih vrednotiti kot enotno področje. Pri tem je poudarila, da tehnologije, prijazne do zasebnosti, zahtevajo zelo kompleksno načrtovanje in razvoj. Njena zaključna misel je bila, da gresta zasebnost in varnost z roko v roki, saj varni sistemi, ki ne spoštujejo zasebnosti, niso več sprejemljivi. Doseči je treba ravnotežje med zaupanjem, zasebnostjo, novimi tehnologijami in sprejemljivostjo za uporabnika. Za konec je navedla še nekaj novih generacij tehnologij s področja zasebnosti, ki naj bi v prihodnje zagotavljale varnost (Cross-domain, Composite, Adaptable, Standard, Common aproaches with trust establishment).

Herbert Leitold (TU Graz) je v svojem predavanju predstavil projekt STORK[7] in elektronsko osebno izkaznico (*Challenges of eID interoperability: What we learn(ed) from the STORK journey?*). Cilj projekta STORK je vzpostaviti evropsko interoperabilno okolje za elektronsko osebno izkaznico (e-OI), ki bo omogočila državljanom posameznih držav vzpostaviti novo elektronsko poslovanje preko meja svojih držav, kjer veljajo nacionalne osebne izkaznice. V tem projektu sodeluje tudi Slovenija.

Začetki posameznih vlad segajo v pozna devetdeseta leta in začetek novega tisočletja. Tako so s samostojnimi projekti začele Finska, Estonija, Avstrija, Italija in Belgija, ki so s tem postale nekakšni nacionalni otoki za uporabo teh e-OI. Projekti se med seboj razlikujejo po tehnologijah (pametne kartice, mobilne e-OI, "mehki" certifikati, uporabniško ime in geslo), po namenu uporabe (javni in zasebni sektor; zvezna, lokalna in regionalna raven; kot identifikator) in v pravnem pogledu (omejena uporaba identifikatorjev na posameznih področjih). Trditev, da je e-OI primerna za čezmejno rabo, je podkrepil z nekaj konkretnimi primeri rabe:

- mobilnost študentov,
- delavci migranti,
- elektronsko zdravstvo,
- napotki za storitvene dejavnosti,
- selitve,
- socialna varnost in
- še več uporabnih aplikacij v zasebnem sektorju.

Country & sec. level		Token Types			Relation to 1999/93/EC		Token Issuer	
	# of cred.	Smart card	mobile eID	soft.-certif.	qualified cert (signature-cert)	is a SSCD	public sector	private sector
Austria	3	yes	yes	-	all	all	yes	yes (all. qual.c.)
Belgium	1	yes	-	-	all	all	yes	-
Estonia	2	yes	yes	-	all	all	yes	-
Germany	1	yes	-	-	optional	all	yes	(opt. qual.certs.)
Iceland	2	yes	-	-	all	all	-	yes
Italy	2	yes	-	-	all	all	yes	yes (sig.-card)
Luxembourg	3	yes	yes	-	all	all	-	yes
Portugal	1	yes	-	-	all	all	yes	-
Slovenia	3	yes	-	yes	all	yes (QAA 4)	yes	yes
Spain	1+80	yes	-	yes	yes (QAA 3-4)	yes (QAA 4)	yes (QAA 3-4)	yes (QAA 3-4)
Sweden	12+	yes	-	yes	-	tbc	yes	yes

Slika 3: Sodelujoče države v projektu STORK

Za uspešen razvoj e-OI so potrebni pilotni projekti v realnih okoljih. Na sliki 3 so naštete države, ki sodelujejo pri pilotnih projektih STORK v prvi fazi razvoja e-OI.

Pri STORK-u ne želijo spremeniti položaja držav članic, ampak si prizadevajo dodati interoperabilnost posameznim projektom:

- Tako imajo države članice svoje projekte osebnih izkaznic (e-OI) in jih načrtujejo, uvajajo ali so že v uporabi.
- Pri tem vsaka država: a) uporablja svojo tehnologijo (pametne kartice, uporabniško ime in geslo); b) svoj način (npr. centraliziran, decentraliziran) in c) svoj pravni okvir (npr. trajni identifikatorji, področno določeni ID-ji).

V prihodnje je treba doseči soglasje o pravnem statusu (članice lahko omejijo uporabo nacionalnih identifikatorjev ali prepovejo čezmejno uporabo identifikatorja), varstvu podatkov (obdelava podatkov mora biti legitimna), odgovornosti (kaj, če gre kaj narobe?) in stopnji zaupanja (akreditacije, samoocenjevanje).

Pilotni projekti:

1. čezmejno preverjanje pristnosti,
2. varnejše klepetanje (varne povezave med otroki),
3. osebne izkaznice za boljšo mobilnost študentov (s svojo študentsko izkaznico se identificirajo tudi v tujini),
4. e-OI za čezmejno dostavo elektronskih nakupov (spletno nakupovanje),
5. spremembe naslova državljanov EU.

Pri STORK-u predpostavljajo, da imajo vsi državljani spletni dostop do e-OI, ki jo je možno uporabiti na različne načine: za identifikacijo (dostop do spletnih storitev), za prenos atributov (STORK opredeljuje e-OI kot identifikator, npr. nacionalna osebna izkaznica, drugi podatki, kot so ime, datum rojstva, izobrazba, pa so atributi), za preverjanje atributov in za preverjanje certifikatov (za elektronski podpis).

V nadaljevanju je predavatelj predstavil še dva pilotna projekta o interoperabilnosti –Middleware (MW) in Pan-European Proxy Services (PEPS), ki ju bodo proučili v okviru projekta STORK. Skupne specifikacije so bile oblikovane tako, da osnovni elementi delujejo na istih protokolih, ne glede na izbiro modela ali njuno kombinacijo. Za lažjo predstavo je navedel težave, ki se pojavljajo pri uporabi različnih električnih omrežij, a jih preprosto rešimo z vmesnimi moduli.

Vloga okolja STORK bo identifikacija uporabnika, ki želi opraviti neko elektronsko storitev pri ponudniku te storitve, in posredovanje podatkov o uporabniku, potrebnih za izvedbo te storitve. Uporabniki bodo imeli stalno kontrolo nad posredovanimi podatki, saj bo vsako pošiljanje podatkov zahtevalo njihovo soglasje. V tem okolju se osebni podatki ne bodo hranili, zato jih ne bo možno izgubiti. Takšen uporabniško orientiran pristop je bil potreben in sprejet zato, da je v skladu z zakonskimi zahtevami vseh vključenih držav, ki se zavezujejo, da bodo s konkretnimi ukrepi zagotovile spoštovanje temeljnih pravic državljanov, kot je zasebnost.

Timothy Edgar (The White House) je predstavil stališča ameriške vlade glede zaupanja vrednih identitet na spletu (*National Strategy for Trusted Identities in Cyberspace – NSTIC*[8]). Na začetku je omenil, da se predsednik Obama v veliki meri zavzema za varnost v celotnem kiberprostoru. Kiberprostor je prostor, v katerem poteka izmenjava informacij, trgovina z različnimi izdelki in različne storitve. Ta prostor tudi omogoča številne druge vrste poslov na številnih področjih in vključuje spletna omrežja naših domov, podjetij, šol in preostale nacionalne infrastrukture. Vsi elementi teh tehnologij niso uspeli slediti hitremu razvoju novih tehnologij. Zasebnost in varnost zahtevata velik premik naprej, ker je tehnologija, ki je prinesla veliko družbenih koristi, prav tako na voljo tistim, ki želijo kakor koli škodovati. Za velik korak naprej pri varovanju v kiberprostoru velja izdaja osnutka nacionalne strategije za zaupanja vredne identitete v kiberprostoru (NSTIC).

Predstavniki ameriške vlade menijo, da predstavlja kiberprostor veliko grožnjo, zato je varnost ključnega pomena za uspešnost gospodarstva in varnost države. Zavedajo se, da morajo delovati mednarodno, kar v veliki meri tudi počnejo. Zavedajo se, da mora zasebnost igrati pomembno vlogo v prihajajočih tehnologijah, zato poskušajo pripraviti mednarodne smernice o upoštevanju zasebnosti pri razvoju. Ne želijo uvesti obveznih osebnih izkaznic, ampak želijo svojim državljanom ponuditi možnost izbire različnih možnosti identifikacije. Prav tako ne želijo vzpostaviti le enega centralnega sistema izdajanja e-OI, ampak več različnih zaupanja vrednih okolij, da se ob morebitni zrušitvi enega ne bi podrl cel sistem. Danes se v večini primerov identificiramo z uporabniškim imenom in geslom, kar je dokaj nezanesljivo (e-pošta, spletno bančništvo, računalniki ...). Menijo, da bi z novimi varnostnimi ukrepi in novimi tehnologijami lahko začeli uporabljati nove spletne storitve za opravila, ki smo jih do sedaj lahko realizirali le tako, da smo bili fizično prisotni. Trenutno je v ZDA za identifikacijo največkrat uporabljeno vozniško dovoljenje, s katerim se državljani lahko identificirajo na različnih mestih. Z vozniškim dovoljenjem lahko odprejo bančni račun, najamejo avtomobil, potujejo z letalom in še več. Pri tem posamezna storitev ne pozna podatkov o drugih uporabah vozniškega dovoljenja in drugih transakcijah. Slabost takšne identifikacije je v tem, da se vedno razkrije več podatkov, kakor je potrebno ali jih želimo razkriti. Pri novem sistemu identificiranja si želijo doseči, da ob posamezni identifikaciji uporabniki razkrijejo le najnujnejše podatke. Želijo si tehnologij, ki bodo v svoj koncept v veliki meri vključevale zasebnost in bodo enostavne za uporabo. Dobro bi bilo uporabiti državljanom poznane tehnologije, ki bi zahtevale njihov minimalen napor pri uporabi. Ena možnost bi lahko bili mobilni telefoni, ki so postali vsakodnevni spremljevalci skoraj celotne populacije. Želijo si izgraditi ekosistem identitet (ang. *identity ecosystem*) s pripadajočo infrastrukturo in združiti zasebnost in kiberprostor. Velik poudarek dajejo tudi informiranju in izobraževanju ljudi. Želijo jim pokazati, da lahko z novimi tehnologijami bolje zaščitijo svojo zasebnost.

Predstavil je tudi navidezen primer uporabe nove tehnologije. Posameznik se prijavi v spletno lekarno, pri čemer uporabi digitalno potrdilo, vezano na njegov osebni računalnik. Tam poda zahtevek za izpolnjen recept. S pomočjo novih tehnologij za boljše varovanje

zasebnosti posreduje skrbnik strankinih atributov veljaven dokaz, da je ta oseba starejša od 18 let in je njen recept veljaven. Tehnologija poskrbi, da se pri vseh teh transakcijah ne prenašajo nepotrebni podatki (datum rojstva in podobno) in da skrbnik atributov ne pride do podatkov o tem, katera zdravila je oseba naročila (ne dobi podatkov od servisa, ki ga je uporabnik na spletu uporabil).

Zavedajo se, da bo treba še veliko postoriti za izobraževanje in informiranje celotne populacije, da bodo z novimi tehnologijami znali zaščititi svojo zasebnost. Zasebnost je ljudem pomembnejša od uporabnosti, ekonomije ... Združiti oziroma povezati bo treba zasebnost in zaščito v kibernetiki.

Razvoj novih tehnologij in ekosistema identitet s pripadajočo infrastrukturo nam daje vpogled, kako bodo v prihodnje digitalne identitete pri spletnih storitvah uporabljali posamezniki, ponudniki storitev in druge interesne skupine. Naša odvisnost od kiberprostora kot sredstva za opravljanje in vodenje poslov ter pretoka informacij bo v prihajajočem obdobju še naraščala, z njo pa tudi potreba po zaupanju identitetam, s katerimi sodelujemo preko spleta. Zaščita identitet posameznikov kakor tudi identitet organizacij pri spletnih transakcijah ima ključno vlogo pri spodbujanju inovativnosti in zaščiti ključnih nacionalnih infrastruktur. Da bo to možno doseči, se morajo vse sodelujoče strani združiti v skupno partnerstvo.

ZAKLJUČEK

Prihajajoče nove tehnologijo bodo v veliki meri vplivale na našo zasebnost, kot je bil to primer Google Buzza, ki so ga sedaj že nekoliko spremenili in izboljšali. Naloga odgovornih institucij je pripraviti novo zakonodajo, s katero bo vsaj do neke mere zaščitena zasebnost posameznika. Z zakonodajo bi morali urediti tudi preostala področja celotnega kiberprostora. Urediti bi morali področje zbiranja podatkov, kdo lahko zbira, katere podatke in s kakšnim namenom. Druga naloga odgovornih je izboljšati informiranost oziroma izboljšati izobraženost celotne populacije, tako da se bodo sami znali bolje zaščititi v kiberprostoru. Danes se veliko uporabnikov kiberprostora ne zaveda, da se zbirajo in hranijo podatki o vseh naših interakcijah in da bodo zaradi novih tehnologij imeli različni ponudniki storitev še boljše možnosti zbiranja še več podatkov, ki bi jih lahko tudi zlorabili.

Zanimiv je primer razvoja mednarodne e-OI v Evropi, s katero bi se lahko uporabniki identificirali na več področjih, med drugimi tudi pri mednarodni izmenjavi študentov, pri spletnih nakupih v drugih državah, kjer ne bi bilo več potrebno predplačilo, kot je to navada pri nakupu preko slovenskih spletnih trgovin. Kar nekaj je bilo tudi govora o spreminjanju dojemanja zasebnosti skozi čas. S prihodom novih tehnologij se lahko to dojemanje zasebnosti spremeni tako, da bo morda nekaj, kar je danes nespremenljivo (sledenje osebam), čez čas povsem normalno in ljudje tega ne bodo doživljali kot poseg v zasebnost.

Nekaj od omenjenih prispevkov bo objavljenih v zborniku referatov, ki ga bo objavila založba Springer predvidoma leta 2011. Prispevki pete mednarodne poletne šole so objavljeni v *Privacy and identity management for life: revised selected papers*.[9]

Opombe

1 http://www.it.kau.se/IFIP-summerschool/
2 http://www.primelife.eu/
3 http://www.jacobhansenshus.se/
4 http://www.androidscience.com/theuncannyvalley/proceedings2005/uncannyvalley.html
5 http://www.google.com/intl/en/about.html
6 http://www.google.com/ads/preferences
7 https://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1
8 http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
9 http://d-nb.info/1003136753/04

Stanislav Pavlič