Storebror på Facebook

– integritet och risker på sociala medier

PÄR STRÖM

PÄR STRÖM

Storebror på Facebook

Integritet och risker på sociala medier

Den Nya Välfärden

den nya välfärden

Box 5625, 114 86 Stockholm
08-545 038 10 | www.dnv.se

Omslagsbild: Salih Güler

Innehåll

Förord 5
1. Det du skriver kan få konsekvenser 6
2. Hur sprids Facebooks information om dig? 16
3. Brottslighet på Facebook 21
4. Polisens användning av sociala medier 24
5. I USA laddar storebror upp 30
6. Ett skräckscenario för framtidens Facebook 38
7. Lagstiftning och reglering av sociala medier 41
8. Facebook som samhällsinstitution 45
9. Checklista för säkerhet på Facebook 47
Källförteckning 50

Förord

Jag tycker själv mycket om Facebook, även om jag valt att inte dela med mig av alla privatlivets detaljer (vilket många gör). Jag är även aktiv på Twitter, och driver en blogg. Jag är alltså verkligen inte negativ till sociala medier.

Att jag skrivit denna skrift beror på att jag ändå ser riskerna, och på att jag tycker mig se att många människor tar otillbörligt lätt på dessa. En godtrogenhet idag kan straffa sig hårt imorgon. De nyheter som lanserades i Facebook hösten 2011 gör att integritetsfrågan hamnar ännu mera i fokus än tidigare.

Med ”Storebror på Facebook” hoppas jag kunna skapa debatt om hur integriteten kan skyddas på de sociala medierna. Jag hoppas också kunna bidra till en ökad försiktighet i användningen av dessa. Utan att därmed döda den fantastiska glädje som de sociala nätverken ger.

Denna skrift finns också i pdf-version som är gratis tillgänglig på www.dnv.se/storebrorpafacebook.

Jag tar gärna emot synpunkter från läsarna på epostadressen par.strom@dnv.se.

Stockholm i oktober 2011

Pär Ström

1. Det du skriver kan få konsekvenser

Nästan alla använder sociala medier – de har blivit en självklar ingrediens i vardagslivet. Facebook har 800 miljoner användare och får 500 miljoner dagliga inloggningar. De sociala nätverken ger oss både glädje och nytta. Många kan numera inte tänka sig ett liv utan Facebook.

Men det finns också en baksida, och dit hör hotet mot den personliga integriteten. Dit hör också risken att utsättas för brott.

Wikileaks-grundaren Julian Assange har sagt att Facebook är en ”spionmaskin”.[1] Alla kanske inte delar den uppfattningen, men gör nog klokt i att iaktta en viss försiktighet i användningen av de sociala medierna. Det är lätt att lägga ut information om sig själv, men ofta betydligt svårare att dra tillbaka den. Och man är aldrig helt säker på vilka händer informationen hamnar i.

Facebooks grundare och huvudägare, Mark Zuckerberg, är känd för att ta lätt på den personliga integriteten. Hans uttalande: ”Just get over it – no one cares about privacy anymore” har blivit bevingat.[2] Uttalandet ska naturligtvis ses mot bakgrund av att Facebook tjänar mer pengar ju mer personliga detaljer människor lägger ut om sig själva. Det beror på att dessa detaljer gör det möjligt för Facebook att erbjuda ännu mer nischade målgrupper till sina annonsörer, vilket höjer värdet på annonsutrymmet.

Intressant nog, och glädjande nog för Facebook, lägger vi ut allt större mängder personlig information. Ribban sänks alltså hela tiden för var gränsen går innan människor tycker att det blir för personligt. Mark Zuckerberg har med anledning av denna trend formulerat det som kommit att kallas Zuckerbergs lag: ”För varje år som går lägger människor ut dubbelt så mycket

personlig information om sig själva som året innan".[3] Inte utan en viss hjälp från honom själv, frestas man tillägga – exempelvis mot bakgrund av nyheterna i Facebook hösten 2011.

Facebook sparar varenda detalj om vad du gör hos dem, förmodligen för all framtid. Allt du skriver, varenda gillning, varenda puffning. Även vänförfrågningar du sagt nej till, vänner du tagit bort, information om vilka vänner som loggat in från samma IP-adress som du (och som alltså varit på samma plats som du), vilka events du bjudits in till, platserna för dessa, hur du har svarat. Och väldigt mycket mer. Information som du har raderat finns också kvar.

Som EU-medborgare kan man begära att Facebook lämnar ut den information de har lagrad om en själv. En kvinna i Österrike som gjorde det fick en rapport på 880 sidor (Se artikeln "Facebook Keeps A History Of Everyone Who Has Ever Poked You, Along With A Lot Of Other Data" i Forbes, 27 september 2011). Om du vill begära ut information om dig själv kan du använda denna länk (som fungerade när denna skrift trycktes): http://tinyurl.com/68et5hc

Farliga nyheter i Facebook hösten 2011

I september 2011 genomförde Facebook en mycket stor omläggning av sin sajt, med både nytt grafiskt utseende och många helt nya funktioner. Flera av nyheterna har en väsentlig påverkan på integriteten, med ökade risker för användarna.

Viktigast ur ett integritetsperspektiv är de nya applikationer (appar) från tredje part som kallas realtidsappar, livsstilsappar eller sociala appar (kärt barn har många namn). Dessa ska ses mot bakgrund av det mycket viktiga faktum att Facebook vill transformera hela mediabranschen så att digitalt material konsumeras *via Facebook*. Lite hårdraget kan man säga att Facebook försöker bli ett nytt eget internet, ett nav för all digital aktivitet. Man ska över huvud taget inte behöva lämna Facebook särskilt ofta.

Facebook vill att människor ska konsumera digitalt material inifrån deras sajt, via de nya realtidsapparna, som är utformade

för att sekund för sekund dela med sig information till vännerna om vad som just konsumeras. Det kan gälla sådant som vilken låt jag just lyssnar på, vilken tidningsartikel eller bok jag just läser, vilket teveprogram jag just tittar på, vilket spel jag just spelar (och mina resultat i spelet), vilken sajt jag just besöker – och så vidare.

”Friktionslös delning” kallar Mark Zuckerberg detta. För Facebook och dess annonsörer öppnas tidigare oanade möjligheter att komma ”under huden” på människor. Visserligen går delningen att stänga av, men den är på i utgångsläget, och grupptryck kan göra att människor låter den vara på.

Synnerligen känslig information

Den typ av information som de nya apparna samlar in är i många fall synnerligen personlig och känslig. Om Facebook-vännerna ser (och Facebook registrerar) att en person läser debattartikeln ”Nationalismen har en viktig roll” (skriven av några sverigedemokrater) så kan det tolkas som att personen är invandringsfientlig – även om hon läser artikeln ur ett kritiskt perspektiv. Över tiden ger det sammantagna valet av artiklar, böcker, filmer, teveprogram, sajter och musik en allt bättre bild av en människas livsstil, intressen, åsikter och värderingar.

Annonsörer är oerhört intresserade av denna skuggbild av människor, eftersom den gör det möjligt för dem att rikta sin marknadsföring mot de som är mest köpbenägna. Facebook kommer mycket riktigt att använda dessa personliga data som underlag för automatiska avgöranden om vilka annonser som visas för vilka människor.

En tjänst för videostreamning kallad Netflix, som är tillgänglig inifrån Facebook och tillämpar ”friktionslös delning”, uppger att information om vilka filmer människor tittar på kommer att samlas in från Facebook-användare utanför USA, men inte från amerikaner. Intressant nog hindrar en gammal amerikansk lag om integritet i branschen för uthyrning av videofilmer loggning av amerikaners filmval.[4] Redan på 1980-talet insåg man alltså i USA hur känslig information om människors filmval är.

Ett exempel på hur mediabranschen kan komma att förändras om Facebook får som de vill är att musiktjänsten Spotify inte längre tar emot nya kunder direkt, utan bara via Facebook. Ett antal internationella mediaföretag har redan lanserat appar för att läsa deras artiklar och se deras filmer inifrån Facebook. Inget svenskt exempel på detta är ännu känt, men flera svenska mediaföretag har börjat driva människor till Facebook genom att kräva att de loggar in via Facebook för att kunna skriva kommentarer till mediaföretagets artiklar.

Vad äter du, och var joggar du?

De nya realtidsapparna frågar en gång för alla användaren om lov att samla in uppgifter. Därefter fortsätter insamlandet utan att det märks, tills appen eventuellt avinstalleras av användaren. Detta behandlas närmare i kapitel 2, ”Hur sprids Facebooks information om dig?”.

Apparna begränsar sig inte till att registrera människors konsumtion av digitalt material, en del av dem sträcker sina tentakler ut i människors fysiska liv. Exempelvis är ”Foodspotting” en app som ska användas för att dela ut information till Facebook-vännerna om vilka maträtter man äter. ”Nike+ Running Monitor” är en app avsedd för att dela med sig information om varje joggingrunda, inklusive kartbild och vilken tid man klarade rundan på. Och så vidare.

En annan förändring i Facebook hösten 2011 är införandet av en tidslinje över människors liv, *Timeline*. Den ersätter det som tidigare kallats Profil, och innebär att profilen går från att vara statisk till att visa utvecklingen över tiden.

Tidslinjen blir en historik över Facebook-medlemmens liv. Människor uppmanas att lägga till uppgifter, även bakåt i tiden, om sådant som när de tog körkort, lärde sig ett nytt språk, köpte bil, reste utomlands, tog en examen, förlovade sig, köpte hus, gifte sig, fick barn, skaffade en ny hobby, skilde sig, flyttade, fortbildade sig, låg på sjukhus, blev sambo igen – och så vidare. Även detta innebär förstås ökade möjligheter att kartlägga en människas liv.

Olika slags risker

Låt oss lämna nyheterna i Facebook hösten 2011, och titta på riskerna med sociala medier ur ett övergripande perspektiv. Dessa risker är av många olika slag. Här följer ett förslag på indelning:

- Det man skriver eller i övrigt lägger ut för en liten skara betrodda personer kan få fötter genom att någon av dem sviker förtroendet. Plötsligt dyker informationen upp i en mycket bredare krets.
- Bland vänner och följare i sociala medier kan det dölja sig personer som har ett syfte med att hålla koll på dig – ett syfte som kanske inte ligger i linje med dina egna intressen. Chefen på ditt jobb? Handläggaren på Försäkringskassan? Din expartner som samlar argument inför vårdnadstvisten?
- Om du ofta skriver om vad du gör, lägger upp bilder och låter realtidsappar registrera din mediakonsumtion skapas successivt en detaljerad bild av ditt liv, dina intressen, värderingar, åsikter, relationer med mera. Hur hanterar företaget bakom sajten denna känsliga information, nu och i framtiden?
- Känslig personlig information kan komma i orätta händer genom buggar i systemet och luckor i säkerheten. Hackare kan ta sig in i databasen.
- Applikationer (appar) kan läcka information genom att de är slarvigt programmerade eller genom att de medvetet samlar in mera information än de får lov att göra.
- Via sociala medier kan man bli utsatt för brottslighet, såsom förtal, dataintrång, bedrägerier och stulna finansiella uppgifter.
- Förmodligen känns hotet från främmande makts underrättelsetjänst inte så stort för en genomsnittlig Facebookanvändare i Sverige. Icke desto mindre kan man konstatera att åtminstone amerikansk underrättelsetjänst och försvarsmakt visar stort intresse för sociala medier, och antagligen finns samma intresse i andra (mindre öppna) länder.

En amerikansk undersökning från 2010, där 2000 hushåll tillfrågades om hur de använder Facebook och andra sociala medier, visade att många människor avstår från att använda Facebooks integritetsinställningar för att minimera riskerna. 52 procent av de vuxna användarna har enligt denna undersökning ett riskabelt beteende och publicerar information om sig själva som kan användas mot dem av cyberbrottslingar.[5]

Den som är intresserad av det riktigt otäcka Storebror ser dig-scenariot rekommenderas särskilt denna skrifts kapitel om vad som sker i USA (kapitel 5). Det är där de mest avancerade övervakningsmetoderna diskuteras och planeras, såsom automatisk statlig personlighetskartläggning av människor via deras information på Facebook.

Tänk på din arbetsgivare

Ett grundläggande råd är att inte skriva något i Facebook, Twitter eller ett annat socialt nätverk som arbetsgivaren skulle uppfatta negativt. Att förlita sig på att chefen inte är med på vänlistan och sedan skriva på Facebook att han eller hon är inkompetent är att utmana ödet.

Det finns gott om exempel på att det har gått illa. En man arbetade på Volvo i Skövde, utsänd av ett bemanningsföretag. Han skrev ”En dag kvar på detta dårhus” på Facebook. Volvo betecknade det som illojalt beteende och skickade hem mannen direkt.[6]

En barnskötare som var mycket uppskattad på förskolan där han arbetade gick på timmar men hade chans att få ett längre vikariat och eventuellt därefter en fast tjänst. Då upptäcktes det att han i sin profilbild på Facebook bar en keps med texten ”Porn star”. Föräldrar blev upprörda, och strax stod barnskötaren utan jobb. ”Han är en jättebra barnskötare men texten är inte förenlig med vår verksamhet”, sa vd på förskolan.[7]

En man som var rektor vid Norrlands entreprenörsgymnasium fick sparken efter att det upptäckts att han figurerade på Facebook lättklädd och som medlem i olika grupper med erotisk

anknytning.[8] Uppsägningen har dock överklagats till Arbetsdomstolen, och utslaget hade inte kommit när detta trycktes.

En svensk polis blev av med sitt jobb efter att ha skrivit på sin blogg om brottsoffer och dessutom beskrivit kvinnliga kollegor på ett hånfullt sätt. Han fick dock senare tillbaka sitt jobb efter att ha vunnit i Arbetsdomstolen (men kommer förmodligen att få helt andra arbetsuppgifter än tidigare). Så sent som hösten 2011, när detta skrivs, blev tre personer i Piteå uppsagda från sina jobb efter att ha skrivit hotfullt om sina chefer på Facebook.[9]

Rättspraxis är oklar vad gäller rätten för arbetsgivare att säga upp medarbetare på grundval av vad dessa säger i sociala medier. Anställda i den privata sektorn löper större risk för uppsägning eftersom lojalitetsplikten anses väga tyngre för dem än för anställda i offentlig sektor.

Det finns särskilda programvaror avsedda att hjälpa arbetsgivare att övervaka vad personalen skriver i sociala medier. Syftet är att förebygga eller avslöja personalens publicering av hemlig eller ofördelaktig information om företaget, liksom att mäta den tid varje medarbetare lägger på sociala medier. En sådan programvara är Social Intelligence Monitoring.

Undersökningsföretaget ClearSwift Research gjorde 2011 en enkät där 906 chefer från företag över hela världen fick svara på frågor om personalens användning av sociala medier på jobbet. Det visade sig att 68 procent av cheferna övervakar sin personals användning av sociala medier.[10]

En undersökning som genomfördes 2011 visar på en stor godtrogenhet avseende riskerna med att skriva i sociala medier om chef, kollegor och arbetsgivare. I undersökningen ställdes frågor till personer i åldrarna 16 till 29 år, och det visade sig att 54 procent av dessa brukar skriva om sin chef och sina kollegor i sociala medier.[11]

Tänk på din framtid

Den som vill vara på den säkra sidan bör hålla sig till principen att inte skriva någonting som inte kan läsas av vem som helst

i hela världen, nu och om 50 år, utan risk för problem. En så långtgående försiktighet kan förstås vara svår att upprätthålla i praktiken, men man bör i alla fall tillämpa riskhantering. Ju känsligare information, desto mera återhållsamhet och desto större försiktighetsåtgärder behövs.

Utgå ifrån att internet aldrig glömmer. Lita inte på spärrar och integritetsskydd. Inget är så lättspritt som digital information. Visst går det att radera exempelvis en bild från Facebook, men den kan redan vara kopierad och spridd utom kontroll för den ursprunglige ägaren.

Hur stor risken är att information som du lägger ut komprometterar dig i framtiden beror delvis på vad du heter. Om du heter Karl Karlsson eller Anna Andersson är det svårt för googlare att skilja ut dig från alla andra med samma namn. Om du heter något unikt, däremot, är du oerhört utsatt för googlare.

En gåva man kan ge sitt barn, om man nu tänker ur ett integritetsperspektiv, är att välja ett vanligt namn för honom eller henne. Särskilt om efternamnet är ovanligt. Å andra sidan är naturligtvis ett ovanligt namn bra ur exempelvis karriärsynpunkt, så länge det är positiv information som hamnar på nätet

En del menar att bilder eller statusuppdateringar som idag kan anses vara komprometterande inte kommer att vara det i framtiden, eftersom det kommer att finnas komprometterande information om alla människor. Det återstår att se om det blir så. Jag känner mig inte särskilt övertygad.

Antag att du om 20 år kandiderar till en hög politisk post. Det står mellan dig och en motkandidat, och det är väldigt jämnt mellan er. Plötsligt får media tag i en bild från en studentfest där du dansar lättklädd på ett bord med en flaska i handen. Någon liknande bild på din motkandidat dyker inte upp just då. Alla vet att ungdomar ofta festar och att du är en mycket mognare person idag. Men ändå – är det säkert att människor inte påverkas undermedvetet så att dina chanser försämras?

Det är inte bara i den politiska världen som festbilder, ogenomtänkta uttalanden och liknande kan vara till skada. Redan idag är det en självklarhet att rekryterare googlar kandidater när

en tjänst ska tillsättas. Ju mera ansvarsfull post det handlar om, desto noggrannare lär dammsugningen av internet vara.

Redan 2009 visade en undersökning gjord av webbsajten CareerBuilder att 45 procent av arbetsgivarna gjorde research på sociala medier om kandidaterna när de skulle rekrytera. Av dessa uppgav sig 35 procent ha valt bort kandidater på grund av vad de hittade, exempelvis opassande foton, förolämpande kommentarer om tidigare arbetsgivare eller skryt om droganvändning.[12] Användningen av sociala medier för research lär knappast ha minskat sedan 2009.

Tänk på myndigheter

Man bör också tänka på att myndigheter kan komma att ta del av det som publiceras på sociala medier. Det kan få konsekvenser – vilket det redan finns exempel på.

Exempelvis skrev en kvinna i Ljusnarsberg i Västmanland på Facebook om ett besök ”på tippen” som hon hade gjort, och att hon hade städat ur en lägenhet och tvättat barnkläder. Socialnämnden läste inlägget, vilket var en bidragande orsak till att kvinnans hemtjänst drogs in.[13]

USA ligger före Sverige i användningen av sociala medier, och därifrån rapporteras många exempel på att myndigheter använder Facebook och Twitter för olika former av kontroller. Detta behandlas i kapitel 5, I USA laddar Storebror upp.

Tänk på inbrottstjuvar

Hur smart är det egentligen att skriva på Facebook eller på sin blogg att hela familjen ska åka till Thailand i två veckor? Det signalerar ju att huset eller lägenheten förmodligen står tomt/tom. Visserligen finns hittills inga belägg för en koppling mellan Facebook och inbrott[14], men det kan komma att ändra sig snabbt.

Flyktingspionage?

Alexander Louhichi, Invandrare för Sverige, skrev i början av 2011 på sin blogg[15]:

> *”För ett tag sedan lade jag märke till en användare på Facebook som jag accepterat som vän. Vi har ett tjugotal gemensamma vänner men ingen kände denna person. Efter en tids undersökning fann jag både profilbilden och bakgrunden vara påhittad. Polisen ser Facebook som ett verktyg för att spana och koppla in nätverk hos misstänksamma personer.*
>
> *Avsändaren som jag fann påhittad hade över 90 procent utländska vänner från olika umgängeskretsar och använde sig av ett mailupplägg som endast tjänstemän använder sig av. Mina misstankar kretsar inte runt någon speciell myndighet men jag har öppnat ögonen för många runt om i Kalmar gällande denna sak.”*

Blogginlägget bevisar förstås inte någonting men stämmer onekligen till eftertanke.

2. Hur sprids Facebooks information om dig?

Facebooks officiella policy för informationsutlämning

I början av hösten 2011 svarade Facebook på ett antal frågor från de nordiska ländernas respektive myndigheter för dataskydd (Datainspektionen och dess motsvarigheter). Frågorna och svaren finns i sin helhet tillgängliga som ett pdf-dokument på det norska Datatilsynets webbplats.[16]

Här redovisas några av de viktigaste beskeden:

- Den information om användare som Facebook kan komma att lämna ut till affärspartners är namn, eventuell profilbild, eventuell tillhörighet till nätverk, användar-id och eventuellt användarnamn.
- Adress, epostadress, födelsedatum och annan information som användaren kan tänkas lägga in i sin profil lämnas inte ut av Facebook till affärspartners, om inte användaren uttryckligen går med på det i samband med installation av en tredjepartsapplikation (alltså en app).
- Facebook lämnar inte ut information till affärspartners om vad medlemmar skriver i sina statusuppdateringar. Foton och filmer lämnas inte heller ut till affärspartners.
- Annonsörer får ingen information om enskilda användare. Däremot används exempelvis statusuppdateringar, ”gillningar” och annan information om aktiviteter på Facebook som underlag för vilka annonser som visas för en viss användare.
- Facebook underkastar sig europeisk dataskyddslagstiftning, vilket bland annat innebär att företaget föresatt sig att följa reglerna i EU:s dataskyddsdirektiv på det sätt som detta har

implementerats på Irland (vilket är det land där Facebook har sitt europeiska huvudkontor).

Läs också den integritetspolicy som finns publicerad på Facebooks webbplats. Det är viktigt att vara medveten om att den kan ändras, och att den historiskt har genomgått stora och snabba förändringar – ofta till integritetens nackdel. Observera också att polisens tillgång till information från Facebook inte omfattas av ovanstående begränsningar. Hur det är med underrättelsetjänster vet vi i princip ingenting om. I Sverige är det sannolikt att FRA:s övervakning omfattar sociala nätverk, eftersom de har mandat att övervaka människors surfande.

Med anledning av att en svensk Facebook-app har läckt information om användare (se nästa stycke) kontaktade jag Facebooks talesman för Norden, Jan Fredriksson, för besked om appars tillgång till personliga uppgifter. Enligt honom får en app bara samla in så mycket information från användarna som krävs för att appen ska fungera – det står i applikationsutvecklarens avtal med Facebook. Facebook verkar dock inte göra någon heltäckande teknisk kontroll av att appar inte samlar in för mycket data, utan förlitar sig på att applikationsutvecklarna följer villkoren i avtalet. Om det kommer till Facebooks kännedom att en app samlar in mer data än den får stängs appen genast av. Vid installation av en app godkänner användaren insamling av den information som appen uppger att den kommer att samla in.

Facebook läcker påfallande ofta

I det förra stycket redovisades vilken policy Facebook har för sin medvetna utlämning av information om användarna till tredje part. Ett stort antal gånger har dock buggar och andra säkerhetshål uppenbarats i Facebooks system, vilket har gjort att information som skulle varit skyddad har kunnat spridas till obehöriga. Här redovisas några exempel på detta, liksom på hur Facebooks data även på andra sätt har samlats in av tredje part på ett sätt som inte varit planerat.

Låt oss börja med en svensk läcka. Inför riksdagsvalet 2010 lanserades en app för Facebook med namnet ”Riksdagsvalet 2010”. Bakom den stod en privatperson. Genom att använda appen kunde man delta i ett slags provval som skulle bidra till att förutse valresultatet. Vid installation av appen godkände Facebook-användarna att vissa typer av information samlades in av den, bland annat epost-adress. Registret med alla app-användarnas epostadresser fick senare spridning och kom att användas för spam.[17] Det är illa nog, men det hade varit ännu värre om även partisympatierna hade spridits, kopplade till respektive epostadress.

Från utlandet finns många Facebook-läckor att rapportera om. Så avslöjades exempelvis 2008 ett säkerhetshål som gjorde det möjligt för utomstående att se andra Facebook-medlemmars fotoalbum – även om de hade ställt in sina integritetsinställningar så att det inte skulle vara möjligt.[18]

År 2010 upptäcktes ett säkerhetshål som gjorde att obehöriga kunde ta del av privata chattar på Facebook, samt se och svara på andra människors vänförfrågningar.[19] Via ytterligare ett säkerhetshål visade det sig vara möjligt för vem som helst att ta del av statusuppdateringar.[20] Ett annat säkerhetshål gjorde det under en period möjligt för utomstående att skriva statusuppdateringar på vissa Facebook-användares konton.[21] Det har också förekommit ett säkerhetshål som i en del fall gjorde det möjligt för företag som annonserar på Facebook att komma åt användares privata information såsom profiler, bilder och meddelanden.[22]

Vissa Facebook-användare kan upptäcka sin profilbild på en dejtingsajt. Dejtingsajten Lovely Faces tog nämligen utan tillstånd 1 miljon profilbilder från Facebook. Av dessa användes 250.000, tillsammans med personliga detaljer om de aktuella Facebook-medlemmarna.[23]

Besökta sajter loggas

Hösten 2010 avslöjades det att ett stort antal av de populäraste Facebook-applikationerna läckte personlig information om

Facebook-medlemmar till både annonsörer och analysföretag. Exempelvis läckte spelet Farmville. Miljontals användare ska ha drabbats, oavsett hur de ställt in sina integritetsinställningar.

Det som kom ut var namn, användar-id (det unika nummer som varje användare har på Facebook) och, för vissa applikationer, namn på vänner. Applikationerna är utvecklade av andra företag än Facebook, som antingen slarvat eller inte följt avtalet med Facebook.[24] Via Farmville har användare också lurats att lämna ifrån sig sitt lösenord till Facebook. [25]

Under 2010 hittades också en bugg i Facebook som gjorde det möjligt för spammare att samla in namn och bilder på Facebook-användare.[26]

En australisk internetentreprenör upptäckte hösten 2011 genom teknisk analys att Facebook loggar sina medlemmars besök på andra sajter, när dessa har Facebook-relaterade funktioner, även när medlemmarna inte är inloggade på Facebook. Det gäller sajter som har en gilla-knapp, en dela-knapp eller en annan Facebook-widget. Normalt inaktiveras så kallade cookies (som kan spåra surfande) när man loggat ut från en sajt, men Facebooks cookies förblir aktiva.

Detta är visserligen inte en läcka i formell mening, men det är informationsinsamling i det tysta som går längre än vad Facebook deklarerat. Företaget har svarat att loggningen inte syftar till att samla in information om medlemmarnas surfande, utan bara görs för att skydda medlemmarna mot spam och nätfiske.[27] Facebooks loggning av utloggade medlemmars surfande kan dock strida mot svensk lagstiftning om cookies, enligt Dagens Nyheter (”Facebooks nya spårning strider mot svensk lag” 29 september 2011).

Man kan konstatera att den som känner till vilka sajter en människa besöker över tiden ofta kan skaffa sig kunskap om den människans livsstil, intressen, åsikter, hälsa – med mera. Surfande är mycket känslig information.

Etisk attack

En expert på datasäkerhet genomförde en intressant demonstration för att påvisa integritetsriskerna med Facebook. Han skrev en liten programvara som samlade in användaruppgifter om 100 miljoner Facebook-användare. Det rör sig om uppgifter som inte var dolda i respektive användares integritetsinställningar.

Den listan ligger nu på nätet som en nedladdningsbar fil. Den innehåller URL (webbadress) till varje användares Facebook-profil, deras namn och unika ID-nummer på Facebook. Även annan information hade kunnat ingå i datainsamlingen, men togs inte med eftersom det ju rörde sig om en ”etisk attack”.[28]

Den här skriften handlar till största delen om Facebook, eftersom det är störst och viktigast av de sociala nätverken. Problemet med integritetsrisker och säkerhetsluckor är dock i huvudsak detsamma för alla sociala nätverk. Exempelvis visade sig mikrobloggen Twitter för några år sedan ha en säkerhetslucka som gjorde att så kallade direktmeddelanden (bara avsedda för en viss person) dök upp i det normala Twitter-flödet som alla kan läsa.[29]

Även säkerhetshål som ligger utanför de sociala nätverken kan göra att människors informationssäkerhet på dessa sätts ur spel. I slutet av 2010 kom exempelvis hackarverktyget Firesheep, ett tilläggsprogram till webbläsaren Firefox, som gjorde det enkelt för bedragare att komma över människors lösenord till olika internettjänster när inloggning gjordes via okrypterade trådlösa nätverk.

3. Brottslighet på Facebook

Sociala medier, och i synnerhet Facebook, har blivit en viktig tummelplats för allehanda brottslighet. Det är inte så konstigt – där människor finns begås det brott, så har det alltid varit, och det finns som sagt nästan en miljard människor på Facebook numera.

Brottsligheten på Facebook får olika konsekvenser för olika aktörer. För den enskilde gäller det att skydda sig mot brott – och för polisen och andra rättsvårdande instanser gäller det att hinna med att bevaka Facebook likaväl som de bevakar gator och torg.

Brottsligheten på Facebook befinner sig i snabb ökning. Under de fem första månaderna 2011 har svensk polis fått in 993 anmälningar om hot eller förtal på Facebook, vilket ska jämföras med 1554 anmälningar för hela 2010. Ser man till helår har antalet polisanmälningar fyrdubblats under de senaste tre åren.[30]

Hot och förtal är dock inte de enda brottstyper som förekommer på Facebook. Enligt polisen fördelar sig de sju vanligaste anmälda brottskategorierna på Facebook så här [31]:

- Kapade konton: 24 procent
- Ofredande: 19 procent
- Förtal och förolämpning: 19 procent
- Olaga hot: 17 procent
- Misshandel: 6 procent
- Sexualbrott: 5 procent
- Övriga: 10 procent

Vissa av dessa brott, såsom misshandel och sexualbrott, initeras förstås bara på Facebook i form av kontaktskapande och fullbordas vid ett senare fysiskt möte. Man kan naturligtvis diskutera om en misshandel som har föregåtts av en kontakt på Facebook ska betecknas som Facebook-brottslighet.

Kapade och falska konton

Den vanligaste typen av brott på Facebook är alltså kapade/falska konton, vilket innebär bedrägerier med dataintrång som en ingrediens. Det kan röra sig om att öppna ett konto i någon annans namn och sedan utge sig för att vara den personen, vilket exempelvis kan utnyttjas för att lura till sig pengar från vänner till den person vars namn har använts. Det kan också röra sig om att ett befintligt konto kapas, kanske genom att lösenordet stjäls.

Svenska Dagbladet berättar om ett aktuellt fall. ”Håkans” Facebook-konto togs över av en okänd person, som använde det för att be Håkans vänner om att få låna pengar. Bland annat påstod bedragaren att Håkans flickvän var inlagd på sjukhus. En av vännerna förde över 32 000 kronor till bedragarens bankkonto.[32]

När det gäller olaga hot på Facebook är hälften riktade mot minderåriga, och just ungdomar återkommer generellt sett något oftare än andra grupper. En av polisens ungdomsutredare berättar att anmälningarna om hot på Facebook sällan är enskilda incidenter utan ingår i ett större sammanhang. Ungdomsutredaren säger också att hoten på Facebook sällan eller aldrig förverkligas.[33]

Något som underlättar brottslighet på Facebook är möjligheten att vara anonym. Såvitt känt föreligger inga planer från företagets sida att avskaffa möjligheten till anonymitet. Visserligen måste för- och efternamn anges av den som vill öppna Facebook-konto, men det sker ingen kontroll av att namnet stämmer med personen.

Mörkertalet avseende brott på Facebook anses vara stort. Bland annat säger Johanna Östergren, som är kurator på ungdomsmottagningen i Huddinge kommun och på kommunens stödcentrum för unga brottsoffer, att bara ett fåtal av de brott som inträffar i sociala medier anmäls.[34]

Skadlig kod sprids

Vissa typer av brott på Facebook blir nästan aldrig polisanmälda. Det gäller exempelvis spridning av skadlig kod. IT-företaget

Cisco förutspådde i sin årliga säkerhetsrapport år 2010 att sociala medier under 2011 skulle komma att bli den viktigaste kanalen för spridning av skadlig kod (såsom virus och trojaner). [35]

Skälet är enkelt. När människor tror att ett meddelande eller en länk har skickats från en Facebook-vän är de inte lika misstänksamma som annars, och därmed mer benägna att vidta åtgärder (såsom att klicka på länken) som kan innebära att skadlig kod installeras på datorn.

Brott på internet möjliggörs ofta av att den drabbade har slarvat med hanteringen av lösenord. Här kan den personliga informationen på Facebook utgöra ett verktyg för bedragaren. Ett exempel ur verkligheten: En 23-åring i USA sökte igenom Facebook efter kvinnor som uppgett sina e-postadresser i sin profil. Han läste respektive kvinnas personliga information, och med den kunskapen kunde han i 46 fall besvara e-postleverantörens så kallade ”hemliga fråga”. Därmed kunde han kapa offrens epostkonton.[36]

I sin säkerhetsrapport från 2010 varnade Cisco också för en ökning av attacker i sociala medier med så kallad social ingenjörskonst som vapen. Det innebär att en bedragare tar kontakt, bygger upp ett förtroende och helt enkelt får offret att frivilligt lämna ut känslig information (såsom lösenord). Bedragarna använder ofta en kombination av charm och förtroendeingivande beteende.

4. Polisens användning av sociala medier

Att polisen finns på Facebook och andra sociala medier är lika naturligt som att de finns på gator och torg. Av hänsyn till den personliga integriteten är det dock av stor betydelse *vad* de gör där, och *hur* de gör det.

Polisiär närvaro i sociala medier kan delas in i tre kategorier, beroende på syfte:

1. Att informera och ha en kontaktyta mot medborgarna.
2. Att förebygga/avslöja brottslighet som begås just i de sociala medierna.
3. Att övervaka de sociala medierna för att i generell bemärkelse bekämpa brottslighet.

Ifall polisen skulle få tillgång till personlig information från Facebook och andra sociala medier som inte är offentlig, utan att det föreligger en brottsmisstanke mot den aktuella personen, skulle det vara ett stort och oacceptabelt intrång i den personliga integriteten.

Däremot är det åtminstone min ståndpunkt att det är helt i sin ordning att polisen ”patrullerar” Facebook och tar del av öppen information – alltså sådant som vem som helst kan ta del av. Det motsvarar polisens patrullerande med bil och till fots på gator och torg.

Bristande resurser

Idag pratas det en hel del om polisiär patrullering på nätet, men åtminstone i Sverige är det mycket snack och lite verkstad. ”Vi har för lite personal för att till exempel spana på Facebook”, säger David Beukelmann, som är chef för ungdomsroteln vid citypolisen i Stockholm. ”Det finns 1100 poliser i city. Men i det virtuella Stockholm är det helt klart glesare, vi hinner inte patrullera på nätet”.[37]

Polisen saknar inte bara personal för att kunna genomföra nätspaning, de saknar också utrustning. Internetuppkopplade datorer är (av säkerhetskäl) bristvara hos polisen, och det har förekommit att poliser måste använda hemmadatorn på kvällen för nödvändig spaning på nätet. När det gäller att säkra bevis på internet eller i beslagtagna datorer är också brist på IT-kompetens inom polisen ett problem. I dagsläget är det alltså inte mycket till internetspaning som genomförs av svensk polis.[38]

Poliser som bland annat Svenska Dagbladet har intervjuat berättar att många unga som befinner sig på glid mot en kriminell värld har öppna profiler på Facebook. Den informationen skulle alltså utan problem kunna användas i brottsförebyggande syfte, exempelvis för att störa nyrekrytering till de kriminella nätverken. Det har visat sig att kriminella element ofta skryter om sina brott på nätet. Det är också vanligt att förövare visar sig vara Facebook-vänner med sitt offer. I båda fall utgör alltså sociala nätverk ett potentiellt kraftfullt verktyg för polisen.[39]

Men polisen har alltså inte tid att gå igenom informationen. ”Nästan all brottslighet går numera att härleda till Facebook. Men vi är inte rustade för den här utvecklingen, den digitala världen har sprungit ifrån oss”, säger Urban Swahn, gruppchef för IT-brottsenheten i Västra Götaland, till Svenska Dagbladet.[40]

Förebyggande terroristjakt

Efter de två terrorattentaten i Norge sommaren 2011 har det politiska intresset för polisiär patrullering av sociala medier

ökat kraftigt. Exempelvis använde ju Anders Behring Breivik sin Facebook-sida för att sprida sitt manifest, och det är naturligt att tankar dyker upp på att kanske kunna hitta framtida terrorister redan innan de hinner slå till. I augusti 2011 sa justitieminister Beatrice Ask till medier att hon vill att polisen ska utöka sökandet på nätet, och att man inom justitiedepartementet för en diskussion om hur det ska gå till.

Det är just våldsbejakande extremism som Ask vill att den polisiära nätspaningen ska vara inriktad på. Så de poliser som vill ha resurser för att via Facebook kartlägga ”vanliga” kriminella verkar inte ha mycket att hämta hos justitiedepartementet – just nu i alla fall.[41]

Från USA rapporterades nyligen att New York Police Department har inrättat en särskild enhet som ska spana på Facebook, Twitter och MySpace. De ska leta efter personer som offentliggör planer på brottsliga handlingar eller skryter om begångna brott i de sociala medierna.[42] Kanske är det den vägen som den svenska polisen med tiden också kommer att gå.

Vid nätspaning är polisens exakta tillvägagångssätt en känslig fråga. Några exempel:[43]

- Om en polis skapar en profil på Facebook för att kunna närma sig ett ungdomsgäng kan det utgöra ett brott mot reglerna för infiltration.
- Om en polis lyckas få en dialog med de potentiellt kriminella kan det komma i konflikt med reglerna för brottsprovokation.
- Om en polis sitter hemma och spanar via sociala medier för att internetuppkopplade datorer saknas på jobbet kan det bryta mot personuppgiftslagen.
- Om en polis gör något med privat utrustning kan det klassas som otillåten privatspaning.
- Om privat utrustning har använts vid spaning kan bevisningen försvåras.

Facebook som bevis

Det finns ett antal exempel på att rättsväsendet i Sverige verkligen har haft nytta av internet. Några exempel: [44]

- I utredningen av den styckmördade Christian Larssons försvinnande i Bollnäs kunde en av de misstänkta gripas efter att han gjort ett inlägg på Facebook.
- I den så kallade kopplerirättegången i Malmö använde åklagaren en statusuppdatering på Facebook som bevisning.
- En man i Lerum som dödade katter och en hund på bestialiska sätt skröt om sina dåd på diskussionsforumet Flashback och lade upp bilder. Polisen kunde spåra honom via IP-adressen.
- I rättegången mot en man i Halland som ägnat sig åt så kallad sextortyr i ett ödehus användes meddelanden mellan mannen och kvinnan på internet som bevis.
- En man som stal en tröja i en affär i Helsingborg kunde gripas efter att personalen känt igen honom på Facebook.

När polisen begär ut data

En viktig och känslig fråga är under vilka omständigheter som Facebook och andra sociala medier lämnar ut icke-offentlig information till polisen. Att ge polisen tillgång till exempelvis statusuppdateringar, vänlistor och meddelanden som en person valt att inte dela med sig av är jämförbart med telefonavlyssning, och det är viktigt att det sker under reglerade former.

Facebooks talesman för Norden, Jan Fredriksson, säger på en direkt fråga att deras policy är att bara lämna ut information om användare när lagen kräver det. Facebook anpassar sig till lokal lagstiftning i respektive land, säger han. Vid varje förfrågan från polisen om utlämning av information kontrollerar Facebook, enligt Fredriksson, om de är skyldiga att lämna ut informationen. I praktiken innebär det att det måste röra sig om ett grovt brott. Jan Fredriksson säger att svensk polis kommer med ungefär en förfrågan i månaden.

Facebook har en officiell (engelskspråkig) sida med information om hur de samarbetar med ”law enforcement”. Formuleringarna där stämmer i huvudsak med det som Jan Fredriksson säger, men är inte lika absoluta. Facebook verkar enligt dessa formuleringar inte helt utesluta utlämning av information till polisen utan att det krävs av lagen.[45]

Beta-test av en ryggrad

Apropå detta är det av intresse att citera en rapport från det amerikanska justitiedepartementet med titeln ”Obtaining and Using Evidence from Social Networking Sites”. Där redovisas vilket förhållningssätt olika sociala nätverk har till polisens önskemål om utlämning av information. I rapporten framställs Facebook som mycket mera samarbetsvillig än Twitter. Det står bland annat att Facebook var ”often cooperative with emergency requests”.[46]

Justitiedepartementet klagar däremot på Twitter, som ”requires a search warrant for private messages/bulletins less than 181 days old”. Det klagas också på att Twitter ”will not preserve data without legal process” och på att Twitter har en ”stated policy of producing data only in response to legal process”. Facebook har protesterat mot rapportens antydan att de lämnar ut data om användare utan laglig grund.

Twitter har också i ett annat sammanhang fått beröm för sitt värnande om användarnas personliga integritet. I samband med de känsliga läckorna av bland annat diplomatiska samtal på sajten Wikileaks begärde amerikanska myndigheter ut personuppgifter från Twitter om några twittrare som förmodades ha varit delaktiga i Wikileaks arbete. Det gällde bland annat Wikileaksgrundaren Julian Assange, den misstänkta läckande militären Bradley Manning, den tidigare talespersonen för WikiLeaks Birgitta Jonsdottir och WikiLeaks-aktivisten Jacob Appelbaum.

En domstol beslutade att Twitter var tvunget att lämna ut informationen. Dessutom belade domstolen företaget med yppandeförbud, vilket innebär att Twitter inte fick berätta att begäran hade kommit och att informationen skulle lämnas

ut. Twitter överklagade yppandeförbudet i domstol och vann. Därmed kunde företaget offentliggöra utlämnandet av personuppgifter, vilket bland annat gav de drabbade användarna ett visst tidsutrymme för att överklaga domstolsutslaget om informationsutlämning.[47]

Tidningen Wired är full av beundran. De skriver:

> *”Förra månaden introducerade Twitter en ny funktion utan att berätta för någon om det, och resten av IT-världen borde ta intryck av det och komma med en egen version. Twitter betatestade en ryggrad.”*

Tidningen skriver vidare att Twitters agerande borde vara branschstandard.

Vill myndigheten ”adda” dig som vän?

En viktig fråga är förstås om polisen och andra myndigheter nöjer sig med att studera öppen information i sociala medier, alltså sådant som människor valt att hålla tillgängligt för alla, eller om de försöker bli ”vän” med människor för att komma åt icke-offentlig information. I det senare fallet går en viktig principiell gräns mellan att bli vän under riktig och påhittad identitet. Full öppenhet kräver förstås, om myndighetspersonen använder sitt verkliga namn, att han eller hon gör klart att vänförfrågan sker i tjänsteutövande syfte.

I Sverige finns såvitt känt inga tecken hittills på att kontrollinstanser använder sociala medier under falsk identitet. I USA, däremot, verkar detta vara utbrett (se nästa kapitel).

Det går förstås att komma åt människors privata information i sociala medier på andra sätt än genom att bli ”vän” med dem, exempelvis med tekniska metoder eller genom att sätta press på nätverksföretagen. Då är vi inne på vad som motsvarar telefonavlyssning liksom på underrättelseinhämtning (spionage) och den verksamhet som FRA bedriver i Sverige.

5. I USA laddar Storebror upp

Det kan vara intressant att studera hur man förhåller sig i USA till användning av sociala medier för polisiär verksamhet, övervakning och kontroll. Det som sker i USA idag kommer ju ofta till oss imorgon.

Sammanfattningsvis kan sägas att medvetenheten hos myndigheter och andra kontroll- och övervakningsinstanser om möjligheterna med sociala medier verkar vara betydligt större i USA än i Sverige. Exempelvis visar skatteverket, immigrationsverket, underrättelsetjänsten och militären stor aktivitet på området, förutom polisen. Går man efter olika forskningsprojekt som finns beskrivna framtonar föraningar om ett rent George Orwell-samhälle.

Många intressanta och avslöjande dokument har kommit i offentlighetens ljus genom att medborgarrättsorganisationen Electronic Frontier Foundation (EFF) gått till domstol och begärt ut handlingar med stöd av en lag kallad ”Freedom of Information Act”. Det gäller exempelvis en pm från det amerikanska immigrationsverket (U.S. Citizenship and Immigration Services) med titeln ”Social Networking Sites and Their Importance to FDNS”. FDNS ska uttydas ”Office of Fraud Detection and National Security” (alltså ”Myndigheten för upptäckt av bedrägerier och nationell säkerhet”).

Utnyttja ”narcissistiska tendenser”

I detta dokument, som riktar sig till myndighetens personal, står det:

> *”Narcissistiska tendenser hos många människor driver dem att vilja ha en stor grupp av ‘vänner’ länkade till sina sidor och*

många av dessa människor accepterar cybervänner som de inte ens känner. Det skapar en utmärkt utsiktspunkt för FDNS att observera det dagliga livet hos bidragstagare och ansökare som misstänks för bedrägliga aktiviteter. [...] Det sociala nätverkandet ger FDNS en möjlighet att upptäcka bedrägerier genom att titta igenom dessa sajter för att se om ansökande personer och bidragstagare har en verklig relation eller försöker lura CIS [U.S. Citizenship and Immigration Services] angående deras relation."

Sedan skriver de att kontroller via sociala medier är att likna vid "cyberhembesök" hos ansökare och bidragstagare. Lite längre ned i dokumentet följer en instruktion om hur man blir "vän" med en person på ett socialt nätverk, och en lista på olika sociala nätverk. Det står inte i klartext, men formuleringarna kan tolkas som en uppmuntran till medarbetarna att försöka bli "vän" med personer vars fall de håller på att handlägga.[48]

Skattmasen läser Facebook

Electronic Frontier Foundation har också tvingat fram utlämnande av en träningsmanual som det amerikanska skatteverket (IRS) har utarbetat för att lära sin personal att använda sociala medier i yrkesutövningen. Den beskriver många tjänster på internet, alltifrån Facebook till Google Street View, som kan användas av myndigheten vid kontroll och utredning av skattebetalare. Denna manual är integritetsvänlig i så måtto att personalen på skatteverket förbjuds att använda falsk identitet för att bli "vän" med skattebetalare som ska kontrolleras eller undersökas.

Trots denna inskränkning finns det mycket att hämta på Facebook för den amerikanska skattmasen. Människor berättar ju i sociala medier om när de flyttar, gör bra affärer, får ett jobb eller uppdrag till sin firma – ofta utan att hålla informationen privat. Då läser IRS. Exempelvis lyckades skatteverket bärga 2000 dollar i skatt från en DJ efter att han skrev på MySpace att han fått ett DJ-uppdrag på en stor offentlig fest.

I ett annat fall framgick det att en person som var under skatteutredning, men hade gått under jorden, var verksam som segelriggare (en som arrangerar segel på båtar). Skatteverkets tjänsteman sökte på hans namn tillsammans med termen ”sail rigger”, och hittade ett lokalt diskussionsforum för just segelriggare. I en tråd frågade någon var mannen befann sig, eftersom hans butik var stängd. ”Åh, han har bara flyttat tvärs över bukten”, hade någon annan svarat. Skatteverket hittade mannen och drev in en fyrsiffrig summa i skatt.

Allt detta rapporterar Wall Street Journal.[49] Enligt den artikeln använder skatteverkets indrivare som en första åtgärd Google, och därefter sociala medier och olika chattrum.

Uppmuntras använda falsk identitet

Ett annat dokument som Electronic Frontier Foundation har tvingat fram är en pm från det amerkanska justitiedepartementet med titeln ”Obtaining and Using Evience from Social Networking Sites”. Det är ett internt dokument framtaget av departementets ”Criminal Division”. Dokumentet går igenom ett antal olika sociala medier-företag och redovisar bland annat deras policy kring datalagring och hur de bemöter och handlägger förfrågningar om att lämna ut information till polisen och andra rättsvårdande instanser (det togs upp i denna skrifts kapitel ”Polisens användning av sociala medier”).

Justitiedepartementets pm listar tre skäl för myndighetsrepresentanter att anta en falsk identitet i sociala medier. I texten ställs frågan ”Why go undercover on Facebook, MySpace, etc?”, och den ger tre svar: ”Communicate with suspects/targets”, ”Gain access to non-public info” och ”Map social relationships/networks”.

Det handlar alltså för myndigheterna om att använda falsk identitet för att kommunicera direkt med misstänkta personer, skaffa tillgång till icke-offentlig information och kartlägga människors relationer och vänskapsband.

På ett annat ställe i dokumentet uppmanas myndigheters personal att använda sig av sociala medier för att finna svagheter hos

vittnen som i rättegångar vittnar *mot* staten, och för att i förebyggande syfte hitta tänkbara svaga punkter för vittnen som vittnar *för* staten. En uppmaning är: ”Gör research på sociala medier om alla vittnen” (justitiedepartementets egen understrykning).[50]

Facebook för bakgrundskontroller

Ett dokument från 2008, utarbetat av ”Office of the director of national intelligence” (ODNI), propagerar för att använda information som människor publicerar om sig själva på internet i samtliga former av bakgrundskontroller som myndigheter behöver göra. Det framgår att ”användbara resultat” har nåtts i 53 procent av fallen i en studie där den enda information som fanns som grund för sökningarna var namn, adress, födelsedatum och ”social security number” (ungefär motsvarande personnummer).

Myndigheten fann också att 48 procent av dem som undersöktes hade två eller fler bitar av negativ information om sig själva tillgängliga på internet. Högst var andelen i åldersgruppen 18 till 24 år. Den negativa informationen kunde vara ”överdrivet informativt offentliggörande av personliga data” och arbetsrelaterad information, liksom referenser till illegal användning av droger (inklusive bilder på detta).

Det aktuella dokumentet säger också att det finns en stor nytta för myndigheter i att inhämta information om personer som utreds genom att intervjua deras ”vänner” i sociala nätverk.[51]

Ett annat dokument som har släppts ut är en presentation från ”Drug Enforcement Administration” (DEA). I detta nämns ett exempel där en rymling kunde hittas efter information som fanns i en video som i sin tur hittades genom sökning i sociala medier. I DEA:s presentation behandlas också möjligheten att använda verktyg på nätet som MySpace Visualizer och YouTube Visualizer för att grafiskt åskådliggöra relationer mellan människor (göra vänkartor).

Det verkar också på DEA:s presentation som om de ser mellan fingrarna avseende myndigheters användning av tillfälliga säkerhetshål i olika internettjänster för att komma åt information

som inte är offentlig. I en intressant formulering nämner också DEA möjligheten att ”inhämta ‘privat’ information som bara delas med dem som valts ut av sidans ägare”.[52]

Hemliga konton

Medborgarrättsorganisationen EFF har också tvingat fram ett dokument kallat ”FBI Intelligence Information Report Handbook”. Där nämns ”hemliga konton” som en möjlighet att komma åt skyddad information. Också Secret Service är inne på samma spår i ett framtvingat dokument där de rekommenderar personalen användning av ”fristående datorer” med ”anonyma konton från en internetleverantör” för att inte lämna efter sig några elektroniska fotspår som kan kopplas till organisationen.[53]

Något annat som uppmärksammats i USA är den övervakning av sociala medier som myndigheterna iscensatte inför installationen av Barack Obama som president. Department of Homeland Security skapade ett ”Social Networking Monitoring Center” för att söka efter ”intressanta saker” på sociala medier under den närmaste tiden före installationen. Så kallad trendanalys tillämpades också.[54]

Ett enskilt fall som väckt uppmärksamhet är när en student med ett arabiskt namn i Kalifornien hittade en underlig sak på sin bil, och misstänkte att det var en GPS-spårare. En vän till honom la upp en bild av apparaten på internet. Inom kort dök en grupp FBI-agenter upp och begärde apparaten tillbaka.[55]

Ytterligare ett amerikanskt exempel som kommit till allmän kännedom på användning av falsk identitet i sociala medier kan hämtas från delstaten Massachusetts. Tidningen Boston Globe citerar en distriktsåklagagare i denna delstat som säger att en del poliser regelmässigt ”går undercover” på Facebook som ett led i sina utredningar.[56]

Underrättelsetjänsten CIA har en institution kallad ”Open Source Center”, vars roll är att samla in öppen information från källor på internet såsom bloggar, chattrum och sociala nätverk. Open Source Center är tillgängligt för användning av nästan

15 000 offentliga tjänstemän på lokal, delstatlig och federal nivå.[57]

Automatisk kartläggning av personlighet

I ännu ett framtvingat dokument framgår det att den federala polisen FBI har ett stort intresse för ett projekt från University of Arizona kallat Dark Web Project. Dess syfte är att ”systematiskt samla in och analysera terroristgenererat material på webben”. Information i dokumentet säger att projektet är särskilt effektivt på spindlar som söker igenom internetfora. Inom Dark Web Project utvecklas också ett verktyg kallat Writeprint som ska kunna användas för att identifiera skaparna av anonymt material på nätet.[58]

Den amerikanska avlyssningsmyndigheten National Security Agency (NSA) har finansierat forskning syftande till att utveckla ett system som kan genomföra automatisk kartläggning av människors personlighet i masskala baserat på vad de skriver i sociala medier. Tanken är att också väga in digital information om människors inköp, banktransaktioner och liknande för att optimera skuggbilden.[59] Det finns redan en enklare allmänt tillgänglig tjänst på internet, skapad av en entreprenör, som analyserar en människas personlighet baserat på meddelanden skrivna i Twitter (tjänsten kallas TweetPsych).[60]

Två amerikanska forskare har utvecklat ett system som samlar in data från en människas hela närvaro i sociala medier – Facebook, Twitter, bloggar med mera – och analyserar hur människans känslor och humör varierar över tiden. Systemet kan exempelvis visa att en människa har varit nedstämd det senaste halvåret men nyligen genomgått en förändring till det bättre. Forskarna vill med detta enkla prototypsystem visa att det är möjligt att göra automatisk personlighetskartläggning via sociala medier.[61]

För övrigt har Google ansökt om patent på en teknologi som kartlägger en människas personlighet genom automatisk analys av hennes googlesökningar.[62]

Kartläggning av rykten

Den amerikanska militärens forskningsorganisation Darpa offentliggjorde under 2011 planer på att utveckla ett system för att automatiskt kartlägga vad som händer i sociala medier. Rykten och diskussionsämnen som snabbt växer i de sociala nätverken ska snabbt upptäckas, och systemet ska analysera vem som ligger bakom och om det är ”naturligt” tillkommet eller ett resultat av någon slags organiserad kampanj (från en organisation eller främmande makt).

Bland annat ska systemet upptäcka och följa ”skapande, utveckling och spridning av idéer och koncept”. Det ska hitta främmande makts propagandakampanjer i sociala medier, och dessutom hjälpa USA att själv skapa och lansera sådana kampanjer. Programmet heter ”Social Media in Strategic Communication” (SMISC).[63]

Amerikansk militär har nyligen upphandlat ett system avsett för hantering av multipla onlinepersonligheter. Upphandlingsdokument anger, enligt Washington Times, att systemet ska ”göra det möjligt för en operatör att styra ett antal olika onlinepersoner från samma dator utan risk för upptäckt av avancerade motståndare”. Det står att systemet ”gör det möjligt för en amerikansk militär handläggare att styra upp till tio separata identiteter baserade över hela världen”. Totalt ska 50 amerikanska militärer kunna styra sammanlagt 500 sådana falska internetpersonligheter.[64]

CIA investerar

Ytterligare en indikation på amerikanskt intresse för övervakning via sociala medier är för övrigt att investmentbolaget In-Q-Tel, som utgör en del av underrättelsetjänsten CIA, har investerat i ett bolag med namnet Visible Technologies. Detta företag utvecklar en spindelprogramvara som övervakar vad som sägs i sociala medier.[65]

I september 2010 skrev medier om att president Obamas administration förbereder ny lagstiftning som ska göra det lättare

för polisen och agenter inom ”national security” att söka igenom sociala medier och avlyssna internet och epostkorrespondens. Det handlar om att alla onlinetjänster som möjliggör kommunikation ska vara skyldiga att ha teknisk utrustning som gör det möjligt att uppfylla en order om avlyssning.[66]

En som hyser stor misstänksamhet mot Facebook är som nämnts grundaren av Wikileaks, Julian Assange. ”Amerikansk underrättelsetjänst har egen tillgång till den sociala nättjänsten Facebooks databas, som innehåller gigantiska mängder med personinformation, via ett speciellt gränssnitt”, sa han i maj 2011 till nyhetskanalen Russia Today. Assange hävdar att även Google och Yahoo har skapat direktingångar i datasystemen för amerikansk underrättelsetjänst.[67]

6. Ett skräckscenario för framtidens Facebook

En del av de exempel som presenteras i denna skrift ger inspiration för att måla upp ett ”worst case-scenario” för Facebook som ett verktyg för Storebror. Så här skulle det kunna se ut framöver, om ett par spektakulära terrorattentat har fått politiska beslutsfattare att släppa alla hämningar när det gäller övervakning:

Nästan alla människor i världens utvecklade länder finns med på Facebook. Många av dem lägger dagligen ut detaljerad information om vad de gör på fritiden, på jobbet, och vad de tycker om dagsaktuella händelser. De lägger också dagligen upp bilder och filmsnuttar – på sig själva, vänner, släktingar, arbetskamrater och människor som råkar gå förbi i bakgrunden.

Facebook har sedan länge blivit navet för världens mediakonsumtion. Genom att erbjuda mediahus förmånliga avtal, med stora möjligheter till riktad marknadsföring, har företaget skapat en situation där digitalt material huvudsakligen konsumeras via Facebook. Det gör att företaget känner till vad varje människa läser för tidningsartiklar, tidskriftsartiklar och böcker, liksom vilka filmer och teveprogram hon ser på. Detta ger över tiden kunskap om varje medlems livsstil, intressen, värderingar och åsikter. Denna information får polis och myndigheter tillgång till.

Via GPS i datorer, telefoner och alla andra digitala enheter blir varje meddelande på Facebook automatiskt försett med exakta geografiska koordinater. Det gäller även bilder och filmer. Detta gör det möjligt att veta var människor har varit, var de är och att följa deras förflyttningar – med 10-20 meters noggrannhet.

Med hjälp av Facebooks automatiska ansiktsigenkänning sker automatisk taggning av alla personer på alla bilder och filmer. Det innebär att inte bara den som laddar upp en bild eller en film ger ifrån sig sin geografiska position, utan även alla som är med på bilden.

Automatisk statlig analys

Via lagstiftning har polis och andra myndigheter i de flesta länder fått egen direktaccess till Facebooks hela databas – inte bara den öppna informationen. De kan fritt söka, både i historiken och i nutid. Avancerade programvaror ger därvidlag väldiga möjligheter. Några exempel:

- *Automatisk framställning av kartor som grafiskt visar människors umgängeskrets. Dessa baserar sig inte bara på vilka som är vänner på Facebook (det skulle ge en alltför grov bild), utan även på mönstret för kommunikation människor emellan och vad som sägs i kommunikationen. Samtalsämne och ordval säger ju mycket om hur nära två människor står varandra.*
- *Automatisk framställning av kartor över hur människor har förflyttat sig geografiskt, liksom kartor som visar var människor är just nu (i alla fall vid senaste statusuppdatering).*
- *Möjlighet att automatiskt ta fram en personlighetsprofil för en valfri människa som är med på Facebook, baserat på många faktorer, exempelvis: Vad han/hon skriver på Facebook, vilka han/hon kommunicerar med och har som vänner på nätverket, vilka böcker, artiklar och teveprogram han/hon tar del av, vilka grupper han/hon är med i och hur han/hon rör sig geografiskt.*
- *En programvara övervakar hela befolkningen (förutom de som vägrar Facebook, de övervakas på andra sätt) i förebyggande syfte. Programvaran söker efter tecken på suspekt aktivitet. Många faktorer vägs in, som var och en poängsätts, och varje människa har i varje stund en total suspekthetspoäng. I detta fall har inspiration hämtats från det påbörjade, men*

avbrutna, amerikanska övervakningsprojektet Total Information Awareness (observera att detta har förberetts på riktigt).

- *Försäkringskassan har en egen programvara som automatiskt letar efter fuskare, exempelvis sjukskrivna och förtidspensionerade som i sin Facebook-aktivitet visar tecken på att arbeta. På motsvarande sätt har Skatteverket en programvara som via Facebook-aktiviteter letar efter tecken på skattefusk. Migrationsverket har sin programvara. Och så vidare.*

7. Lagstiftning och reglering av sociala medier

Den enorma betydelse som de sociala medierna håller på att få i det moderna samhället har inte gått den politiska världen förbi. På många håll finns funderingar och förslag på olika former av lagstiftning och reglering. Hur mycket av den varan det blir, och vilken praktisk betydelse som lagstiftningen i så fall får, återstår att se.

EU skärper dataskyddsdirektivet

Inom EU har justitiekommissionär Viviane Reding tagit initiativ till att uppdatera EU:s dataskyddsdirektiv från 1995. I samband med det har hon i nästan hätska ordalag hotat IT-världens giganter, Facebook och Google särskilt omnämnda, med juridiska åtgärder om de inte följer EU:s regler för bland annat dataskydd. ”Ett USA-baserat sociala medier-företag som har miljoner aktiva användare i Europa måste rätta sig efter EU-regler”, har hon sagt.[68]

Arbetet med att uppdatera dataskyddsdirektivet pågår för fullt, och sociala medier (som knappast fanns 1995) befinner sig i frågans epicentrum. Viktigast i EU:s ambition är att upprätta principen ”rätten att bli glömd”, vilket innebär att varje EU-medborgare ska ha rätten – inte bara möjligheten – att få material om sig själv borttaget från sociala medier. Det må vara text, bilder eller annat material.

Redan idag har en EU-medborgare i princip denna rätt, men han eller hon måste då bevisa att borttagandet är nödvändigt. De uppdaterade reglerna ska vända på bevisbördan, är det meningen. Det innebär att Facebook ska vara tvunget att ta bort materialet

på en medborgares begäran såvida företaget inte kan bevisa att kravet på borttagning inte är berättigat.

Enligt tidiga utkast ska EU:s nya dataskyddsdirektiv bland annat kompletteras med följande skydd:[69]

- En breddning av vilka slags dataskydd som ska vara EU-övergripande.
- Medborgare ska ha rätt att enkelt få data raderade, korrigerade eller blockerade (”rätten att bli glömd”).
- Företagen bakom tjänsterna ska tvingas förstärka det tekniska skyddet av den personliga informationen.
- Företagen ska också vara tvungna att informera sina kunder när säkerhetshål uppstår och data läcker ut eller skulle ha kunnat läcka ut.
- Innan företag börjar lagra data om människor ska de vara tvungna att informera kunderna om vad den lagrade informationen ska användas till.

Det bör understrykas att detta är preliminära tankar och att formuleringarna inte är klara.

Viviane Reding har också sagt att hon inte tvekar att ingripa med lagstiftning om de sociala nätverken inte anstränger sig mera för att skydda minderårigas profiler på tjänsterna.[70]

Internetgiganter som Facebook och Google brukar ställa sig mycket negativa till lagstiftning och annan reglering. De brukar åberopa vikten av yttrandefrihet och förespråkar självreglering istället för lagstiftning. I USA har självreglering varit huvudprincipen ända sedan president Clinton slog in på det spåret i början av internetboomen (även om förslag om lagstiftning i USA har börjat komma på senare tid, något som behandlas i nästa underkapitel). Facebooks grundare och huvudägare Mark Zuckerberg är som nämnts känd för att ta lätt på den personliga integriteten.

Vissa bedömare ställer sig tveksamma till EU:s möjligheter att sätta juridisk kraft bakom sina stora ord. Problemet är att de flesta företag som driver sociala medier befinner sig utanför EU:s jurisdiktion, åtminstone avseende huvudkontorets place-

ring. Bland annat har Facebook vägrat att gå med på krav som liknar de ovan nämnda när de ställdes från Frankrike. Måhända är det på det politiska planet som EU har den verkliga makten att påverka internetföretag.

Lagförslag i USA

Även om huvudprincipen i USA som nämnts är självreglering har det på senare tid börjat dyka upp röster som vill reglera sociala medier även där. I Kalifornien har delstatssenatorn Alan Lowenthal lagt ett förslag om lagstiftning som liknar EU:s princip om ”rätten att bli glömd”. Den tänkta lagen går ut på att tvinga alla företag som för kaliforniska konsumenters räkning använder, samlar in eller lagrar onlineinformation att erbjuda en metod för att ställa sig utanför detta [”opt out”]. Förslaget går under benämningen ” ’Do not track’ bill”. Ett antal stora internetföretag, däribland Facebook, lobbar intensivt mot förslaget.[71]

Även ett annat förslag om lagreglering av sociala medier kommer från Kalifornien och avser delstatslagstiftning. Detta lagförslag, som går under namnet ”Social Networking Privacy Act”, började som ett förslag om att sociala medier-företag ska tvingas ta bort information om minderåriga ifall föräldrarna begär det. Förslaget innebär också specialregler för hur minderårigas information ska hanteras. Med tiden breddades förslaget till att även omfatta vuxna, där den viktigaste ingrediensen är att internetföretag ska bli tvungna att på begäran radera all personlig information om en människa 48 timmar efter begäran.

Facebook är starkt negativt. En talesman för företaget har sagt att lagen skulle vara ett allvarligt hot mot Facebooks affärsverksamhet i Kalifornien och mot möjligheten för kaliforniska konsumenter att göra meningsfulla val om sina personliga data. Efter lobbying från nätverksföretaget stoppades förslaget, men det kan komma att väckas till liv för en ny omröstning i delstaten.[72]

Ett annat offentligt initiativ i USA kommer från Federal Trade Commission. De har genomfört en serie rundabordsdiskussioner om personlig integritet för att skaffa sig en bild

av hur nya teknologier suddar ut gränsen mellan privat och offentlig information. Under ett av dessa möten kritiserades sociala nätverk för att inte anstränga sig tillräckligt för att skydda användarnas data.[73]

Andra länder diskuterar reglering

Flera andra länder har också visat aktivitet på området reglering av sociala medier. Några exempel:

- I Tyskland finns ett lagförslag som går ut på att förbjuda arbetsgivare att göra efterforskningar om arbetssökande på sociala medier.[74]
- Den tyske inrikesministern Hans-Peter Friedrich har uttalat sig för avskaffad anonymitet på internet, varvid han primärt verkar ha haft bloggare i åtanke.[75]
- I Australien har en politiker föreslagit en lag om att föräldrar ska kunna kontrollera och censurera vad deras barn skriver på Facebook.[76]
- I Tyskland, Schweiz och Australien har lagstiftare reagerat på att Facebook låter människor ladda upp bilder på (och information om) andra utan deras medgivande. Lagstiftarna säger att Facebook kan bli tvunget att kontakta de berörda personerna innan uppladdning tillåts.[77]
- I Kanada ansåg lagstiftare att Facebook bröt mot landets integritetslagar, och hotade med juridiska åtgärder om företaget inte genomförde förändringar. Några månader senare offentliggjorde Facebook förändringar som uppfyllde lagstiftarnas krav.[78]

8. Facebook som samhällsinstitution

Vissa fenomen i IT-världen växer sig så viktiga att de i praktiken blir samhällsinstitutioner. Exempel på tjänster som är på väg dit, eller kanske redan är där, är Google, YouTube, Skype, Wikipedia – och Facebook.

Vi börjar definitivt närma oss en situation där det är problematiskt för en människa att *inte* vara med på Facebook. Kommunikation sker i allt större utsträckning inom Facebook istället för via ringande, mejlande eller sms:ande. Bara det innebär att Facebook delvis går mot att motsvara vad som förr i världen kallades *Televerket* – en myndighet och ett tungt maktcentrum.

Människor blir också i allt större utsträckning hittade av andra via Facebook. Att avstå från medlemskap börjar likna vad det förr i världen innebar att inte stå med i telefonkatalogen. Om man ska hårdra det hela kan man säga att vi kanske går mot situationen ”Är du inte med på Facebook så finns du inte”.

Om det nu blir så att Facebook dessutom blir navet för konsumtion av media som musik, tidningar, böcker, teve och filmer så stärks företagets position som samhällsinstitution ytterligare.

Att ett enda privat företag har all makt över ett system som är så viktigt för den enskilda människan är inte helt oproblematiskt. Att detta företag finns utanför Sverige, i en annan jurisdiktion, gör problemet större.

Hur kommer Facebook att hantera integritetsfrågan? Hur väl skyddar de medlemmarnas känsliga information? Hur löser Facebook problem med nätmobbning, ryktesspridning och förtal? Sköter företaget sina plikter exempelvis när det gäller att ta bort material som är olagligt i andra länder än USA? Kommer det

amerikanska företaget att respektera andra länders lagstiftning, även när den bygger på värderingar som skiljer sig från dem i USA? Hur hanterar Facebook sin kommersiella makt, som kan komma att bli enorm?

De flesta sociala medier drivs av företag i en jurisdiktion som ligger utanför inte bara Sverige utan även utanför EU. Det innebär att såväl Sverige som EU har begränsade möjligheter att ingripa juridiskt. Om ett dotterbolag finns i vår jurisdiktion kan åtgärder förstås vidtas mot detta, men det är egentligen inte nödvändigt att ha ett sådant dotterbolag. Att använda retorik där man hotar med juridiska åtgärder är lätt, men det kanske i grund och botten är en politisk och marknadsmässig påtryckning det handlar om.

Vad kan vi göra här mot ett företag utanför EU om detta skulle strunta i de lagar vi inför? Ställer man saken på sin spets finns det två verktyg: att tvinga internetleverantörer som verkar här att spärra sajterna, och att strypa det finansiella flödet till sajterna genom att tvång riktas mot banker och andra finansiella institutioner. Båda åtgärderna är drastiska till sin karaktär och förknippade med politiska svårigheter, vilket gör dem svåra att använda. Dessutom finns möjligheter att gå runt åtgärderna, särskilt när det gäller spärrade sajter.

Hittills har vi haft en situation där globalt verksamma IT- och internetföretag strävar efter att uppträda ansvarsfullt och därför varit relativt lyhörda inför juridiska krav från andra länder. Förhoppningsvis fortsätter det att vara så. Men det faktum att sociala medier ligger utanför vår jurisdiktion gör det ännu viktigare för användare att tänka på vad de lägger ut. Informationen står i grund och botten under utländsk kontroll.

9. Checklista för säkerhet på Facebook

Här följer en lista på enkla (och några inte riktigt lika enkla) åtgärder som kan vidtas för att minimera risken att råka illa ut i användningen av Facebook.

- Acceptera bara vänförfrågningar från personer du verkligen känner.
- Skriv inte sådant som kan komma att vändas emot dig eller som kan skada dig om det hamnar i fel händer.
- Ställ in integritetsinställningarna så att du inte delar med dig av information på ett bredare sätt än du verkligen anser vara nödvändigt.
- Välj ett svårgissat lösenord, med många tecken och helst inblandade specialtecken. Ett bra knep är att hitta på en mening och sedan ta första bokstaven i varje ord (”Jag har 1 bil och 2 barn och 4 rum!” blir ”Jh1bo2bo4r!”). Använd inte samma lösenord för flera internettjänster. Byt ut det ibland och dela inte med dig av det. Låt inte datorn minnas dina lösenord.
- Logga ut från Facebook när du inte använder tjänsten, till exempel om du lämnar datorn för att gå på lunch. Observera att det *inte* räcker med att stänga fliken eller ens stänga webbläsaren. Skulle du ha glömt att logga ut med din vanliga dator och befinner dig på resa kan du logga ut din hemmasession från en annan dator (görs under ”Account settings”, sedan ”Security”)
- Var misstänksam när det kommer uppmaningar att klicka på meddelanden och länkar från en ”vän”. Särskilt suspekta

är uppmaningar på engelska av typen ”Hey, take a look at this” eller ”You’re in this video”. Skadlig kod kan ha tagit över din väns konto. Var också extra misstänksam innan du klickar på en förkortad länk.

- Var misstänksam innan du installerar appar/program, inte minst om det gäller spel. Ladda bara ned appar från företag du litar på.
- Om du är inloggad på Facebook och plötsligt får uppmaningen att logga in igen är det stor risk att du har blivit ledd till en falsk sida som kommer att stjäla ditt lösenord.
- Klipp inte ut ett script du har fått och klistra in det i webbläsarens adressfält om du inte är helt säker på vad scriptet (som är programkod) gör. Det är en mycket riskabel handling.
- Ha alltid de senaste uppdateringarna av din webbläsare installerade. För varje säkerhetslucka som upptäcks kommer snart en uppdatering. Se också till att ditt antivirusskydd är uppdaterat.
- Vill du verkligen ha en höjd säkerhetsnivå kan du använda Facebooks tillval att kryptera kommunikationen genom användning av protokollet https. Då blir det exempelvis omöjligt att avlyssna din kommunikation, och stjäla lösenord, även om du använder ett oskyddat trådlöst nätverk. Gå till ”Account Settings”, sedan ”Account Security”.
- En annan säkerhetsfunktion som Facebook tillhandahåller för de säkerhetsmedvetna är engångslösenord som skickas till din mobiltelefon. Dessa är särskilt bra när man använder någon annans dator (med tanke på risken för program som loggar lösenord).
- Man kan också ställa in Facebook så att du får ett meddelande med epost eller sms ifall någon loggar in på ditt konto med en enhet annan än den du brukar använda. Funktionen ger då möjlighet att avsluta den oväntade inloggningen.
- Ifall du upptäcker att ditt Facebook-konto har blivit kapat, gå genast till www.facebook.com/hacked där du ber Facebook att säkra ditt konto.

- Ifall du upptäcker att någon har startat ett nytt Facebook-konto och låtsas vara du, rapportera detta genom att använda funktionen ”Report/block this person”. Facebook kommer att utreda saken.

Vill du ha mera detaljerad och avancerad säkerhetsinformation? Googla fram och ladda ned den kostnadsfria pdf-guiden ”A guide to Facebook Security For Young Adults, Parents, and Educators”. En del av tipsen ovan har hämtats därifrån.

Källförteckning

1 Artikel "WikiLeaks revelations only tip of iceberg – Assange", Russia Today, 2 maj 2011, artikel "Assange: Facebook en skrämmande spionmaskin", Ny Teknik, 2 maj 2011, artikel "Julian Assange: Facebook is an 'Appalling Spying Machine' ", PCWorld, 2 maj 2011

2 Artikel "New EU Privacy Laws Could Hit Facebook", Bloomberg Businessweek, 29 januari 2010

3 Blogginlägg "Zuckerberg's Law of Information Sharing", New York Times blogg Bits, 6 november 2008

4 Artikel "Facebook updates its status: It wants to be an entertainment hub", Los Angeles Times, 23 september 2011

5 Artikel "Facebook Privacy Concerns Don't Stop Risky Behavior on Social Networks", eWeek, 4 april 2010

6 Artikel "Kallade jobb dårhus – mannen fick sparken", tidningen GT, 3 januari 2011

7 Artikel "Hade fel mössa – förlorade jobbet", Aftonbladet, 22 januari 2010

8 Artikel "Sparkad rektor får skadestånd", Norrländska Socialdemokraten, 31 augusti 2010

9 Artikel "Unga aningslösa på Facebook", Ny Teknik, 6 september 2011

10 Artikel "Most bosses monitor or block social-network use at work", The Register, 7 september 2011

11 Artikel "Unga aningslösa på Facebook", Ny Teknik, 6 september 2011

12 Artikel "New Law to Stop Companies from Checking Facebook Pages in Germany", Der Spiegel, 23 augusti 2010

13 Artikel "Skrev om städning på Facebook – blev av med hemtjänsten", Expressen 21 april 2011

14 Artikel "Inga belägg för koppling mellan Facebook och inbrott", Svenska Dagbladet, 4 augusti 2011.

15 http://alexanderlouhichi.wordpress.com/2011/02/06/polisen-ser-facebook-som-ett-verktyg-for-att-spana/

16 Se www.datatilsynet.no, alternativt förkortad direktlänk till pdf-dokumentet: http://tinyurl.com/42ewqdw

17 Bloggpost "Riksdagsvalet 2010 på Facebook slutar i spam relaterat till Bonnier", bloggen "Nikke Index", 24 september 2010, samt samtal med Facebooks talesman i Norden, Jan Fredriksson

18 Artikel "Facebook-foton spreds via säkerhetslucka", E24, 27 mars 2008

19 Artikel "Major Facebook security hole lets you view your friends' live chats", TechCrunch, 5 maj 2010

20 Artikel ”Massiv kritik mot Facebook efter ny miss”, Aftonbladet, 25 maj 2010
21 Artikel ”Facebook täpper till säkerhetshål”, idg.se, 3 februari 2011
22 Artikel ”Facebook slarvar med säkerheten”, Dagens Nyheter, 11 maj 2011
23 Artikel: ”Dejtingsajt stal en miljon profilbilder från Facebook”, idg.se, 8 februari 2011
24 Artikel: ”Populära Facebookprogram läcker information om dig”, idg.se, 18 oktober 2010
25 Artikel ”Tusentals stulna Facebooklösenord ute på nätet”, idg.se, 15 september 2010
26 Artikel ”Bugg i Facebook läcker ut både bilder och namn”, idg.se, 12 augusti 2010
27 Bloggpost ”Logging out of Facebook is not enough”, Nik Cubrilovic’s blogg, 25 september 2011, och artikel ”Facebook criticised for ’tracking’ logged-out users”, The Telegraph, 27 september 2011
28 Artikel ”Details of 100m Facebook users collexted and published”, BBC News, 28 juli 2010
29 Artikel ”Privacy Disaster At Twitter: Direct Messages Exposed (Update: GroupTweet Is Likely Culprit”, TechCrunch.com, 23 april 2008
30 Artikel ”Polisen står handfallen inför brotten på nätet”, Svenska Dagbladet, 2 augusti 2011
31 Avser 165 anmälningar med direkt koppling till Facebook som inkommit till polisen i Stockholm under maj 2011, enligt artikeln ”Här är de vanligaste brotten på Facebook” i Svenska Dagbladet den 3 augusti 2011
32 Artikel: ”Här är de vanligaste brotten på Facebook”, Svenska Dagbladet, 3 augusti 2011
33 Artikel: ”Här är de vanligaste brotten på Facebook”, Svenska Dagbladet, 3 augusti 2011
34 Artikel ”Här är de vanligaste brotten på Facebook”, Svenska Dagbladet, 3 augusti 2011
35 Artikel ”Sociala medier ‘nya hotet’ – så här skyddar du dig”, Dagens PS, 1 juni 2011
36 Artikel ”Sociala medier – det nya hotet”, Tech World, 1 juni 2011
37 Artikel ”Polisen står handfallen inför brotten på nätet”, Svenska Dagbladet, 2 augisti 2011
38 Artikel ”Polisen står handfallen inför brotten på nätet”, Svenska Dagbladet, 2 augisti 2011
39 Artikel: ”Facebook hjälper polisen lösa brott”, Metro, 17 januari 2011
40 Artikel ”Polisen står handfallen inför brotten på nätet”, Svenska Dagbladet, 2 augisti 2011
41 Artikel ”Ask (M) vill låta polisen utvidga sökandet på nätet”, Svenska Dagbladet, 5 augusti 2011
42 Artikel ”NYPD forms new social media unit to mine Facebook and Twitter for mayhem”, Daily News, 10 augusti 2011

43 Artikel ”Felaktig hantering kan göra poliser till brottslingar”, Svenska Dagbladet, 7 augusti 2011
44 Artikel: Facebook hjälper polisen lösa brott”, Metro, 17 januari 2011, artikel ”Fall där Facebook-material har använts i bevisningen”, Svenska Dagbladet, 2 augusti 2011
45 Sida ”How does Facebook work with law enforcement?”, Help Center, www.facebook.com
46 Artikel ”EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites”, Electronic Frontier Foundation, 16 mars 2010, även artikel ”How US Government Spies Use Facebook (Updated)”, ReadWriteWeb (från New York Times), 16 mars 2010
47 Artikel: ”Twitter’s Response to WikiLeaks Subpoena Should Be the Industry Standard”, Wired, 10 januari 2011
48 Artikel ”Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your ‘Friend’ ”, Electronic Frontier Foundation, 12 oktober 2010
49 Artikel ”Is ‘Friending’ in Your Future? Better Pay Your Taxes First”, Wall Street Journal, 27 augusti 2009
50 Artikel ”How US Government Spies Use Facebook (Updated)”, ReadWriteWeb, 16 mars 2010 (från New York Times” och artikel ”EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites”, Electronic Frontier Foundation, 16 mars 2010
51 Artikel ”Government Finds Uses för Social Networking Sites Beyond Investigation”, Electronic Frontier Foundation, 10 augusti 2010
52 Artikel ”Government Finds Uses för Social Networking Sites Beyond Investigation”, Electronic Frontier Foundation, 10 augusti 2010
53 Artikel ”Government Finds Uses för Social Networking Sites Beyond Investigation”, Electronic Frontier Foundation, 10 augusti 2010
54 Artikel ”Feds Scoured Facebook And Twitter For Obama Inauguration Security Threats”, Forbes, 13 oktober 2010
55 Artikel ”Caught Spying on Student, FBI Demands GPS Tracker Back”, Wired, 7 oktober 2010
56 Artikel ”Twitter Tapping”, New York Times, 12 december 2009
57 Artikel ”Government Uses Social Networking Sites for More than Investigations”, Electronic Frontier Foundation, 16 augusti 2010
58 Artikel ”Government Uses Social Networking Sites for More than Investigations”, Electronic Frontier Foundation, 16 augusti 2010
59 Artikel ”Pentagon sets its sights on social networking websites”, New Scientist, 9 juni 2006
60 Bloggpost ”Psychological Profiling Via Twitter”, Dan Zarrella, 15 juni 2009, och själva tjänsten på http://tweetpsych.com
61 Artikel ”New Tool Hacks the Psyche”, Security Darkreading, 14 augusti 2008
62 Artikel ”Forget Demographics Google May Soon Offer Psychological Profiling”, Search Engine Watch, 14 maj 2007

63 Artikel ”Pentagon Wants a Social Media Propaganda Machine”, Wired, 15 juli 2011, bloggpost ”Pentagon Seeks a Few Good Social Networkers”, New York Times, 2 augusti 2011
64 Artikel ”Pentagon buys social networking ’spy software’ ”, The Telegraph, 17 mars 2011, och artikel ”Revealed: US spy operation that manipulates social media”, Guardian, 17 mars 2011
65 Artikel ”Twitter Tapping”, New York Times, 12 december 2009
66 Artikel ”Obama demands online wiretap bill to allow spooks to eavesdrop on BlackBerries and social networking sites”, Daily Mail, 28 september 2010
67 Artikel ”Assange: Facebook en skrämmande spionmaskin”, Ny Teknik, 2 maj 2011, och artikel ”Julian Assange: Facebook is an ‘Appalling Spying Machine’ ”, PCWorld, 2 maj 2011
68 Artikel ”Facebook and Google ‘must follow’ EU privacy rules, ZDNet UK, 17 mars 2011
69 Artikel ”EU takes on Internet giants”, The Prague Post, 17 augusti 2011, och artikel ”Facebook and Google Face New Data Regulations, EU Demands”, Silicon Angle, 16 mars 2011
70 Artikel ”Facebook under privacy microscope”, Financial Times, 11 april 2010
71 Artikel ”Google, Facebook: ”do not track” bill a threat to California economy”, Ars Technica, maj 2011, och artikel ”Web tracking bill draws fire from Facebook, Google”, MarketWatch, 3 maj 2011.
72 Artikel ”California Bill Would Force Change to Facebook Privacy Settings”, Reuters, 16 maj 2011, artikel ”Facebook lobbied to kill bill aimed at social media”, USA Today, 12 januari 2011, och artikel ”Web Giants Bust the Social Networking Privacy Act”, Hubze, 8 juni 2011
73 Artikel ”Facebook under privacy microscope”, Financial Times, 11 april 2010
74 Artikel ”New Law to Stop Companies from Checking Facebook Pages in Germany”, Der Spiegel, 23 augusti 2010
75 Artikel ”Tysk minister vill att bloggare kliver fram”, Svenska Dagbladet, 7 augusti 2011
76 Artikel ”South Australian politician wants law to allow parents to censor their kids’ Facebook profile”, CNN Go, 16 juni 2011
77 Artikel ”Facebook under privacy microscope”, Financial Times, 11 april 2010
78 Artikel ”Facebook under privacy microscope”, Financial Times, 11 april 2010

Utgivet av Den Nya Välfärden

Storebror på Facebook – integritet och risker på sociala medier (2011)
Sex feministiska myter – sann jämställdhet kan bara byggas på sanningens grund (2011)
Skatteprocessen hotar rättssäkerheten (2010)
Låt dem inte komma undan – tio viktiga frågor till Sveriges politiker (2010)
Arbetslöshetens rätta ansikte (2010)
Kommunala bolag – laglöst land (2009)
Bara företagare skapar nya, riktiga jobb (2009)
Storebror tar fram munkaveln
– internetfiltrering – censur som hotar yttrandefriheten(2009)
Hälso- och sjukvårdsföretagsmodellen (2009)
Den Nya Välfärdens arbete gör nytta för pengarna (2008)
Olagligt billigt – kommunala underprisförsäljningar (2008)
Integritetens lilla röda (2008)
Regeringen har fel om arbetsrätten – företagarnas egen uppfattning (2008)
Förenkla reglerna för småföretagare (2007)
Den stora obalansen – hur lagarna missgynnar småföretagare (2007)
Varför straffa den som försöker göra rätt (2007)
Värsta krånglet (2007)
Mansförtryck och kvinnovälde (2007)
Fullt fokus på företagare
– europeiska företagare ger råd till Sveriges regering (2007)
Med storbror i byxfickan – integritetsrisker med RFID-chips (2007)
Roligt värre (2007)
Med storbror i uppfinnarverkstan
– ny digital övervakning från automatiska öron till internetdammsugare (2006)
Med storebror i baksätet – digital övervakning av dina bilfärder (2006)
Nya beska droppar – korta kritiska krönikor (2006)
Första hjälpen
Om dina anställda blir sjuka – en liten handbok (2006)
Var tredje får inte vara med
– en studie om arbetslösheten bland invandrare (2006)
Hur hög är arbetslösheten, egentligen? (2006)
Ole, dole, arbetslös
– nästan 3 av 10 ungdomar 16-24 år saknar jobb (2006)
Ge de arbetslösa en chans
– 150 000 nya jobb genom halverade arbetsgivaravgifter (2006)
Så lyckas du som företagare
– de bästa tipsen från svenska entreprenörer (2005)
Bakom skurkar och skandaler (2004)
Värsta krånglet (2004)

Jobbet är att mata puman
– hur och varför försäkringskassorna slarvar bort 40 miljarder om året av skattebetalarnas pengar (2004)
Tankebok för entreprenörer
– 222 citat från Aristoteles till Ingvar Kamprad (2003)
Entreprenören bakom allt
– 101 svenska succéer från ABBA till ölburkar (2002)
Beska droppar – korta kritiska krönikor (2002)
Skärp dig, Svensson
– med deklarationen om medborgerliga skyldigheter (2002)
Personvalsparti – bot för trötta partier (1999)
Berättelsen om jobben (1996)
Baksmällan – förutsättningar för politisk tillnyktring (1995)
Molnstoden – en vision för svenska folket (1994)

Den Nya Välfärden har även givit ut Medborgarnas Offentliga Utredningar

MOU 2010:1 Trovärdig solidaritet – försvaret och solidaritetsförklaringen
MOU 2000:1 Sveriges två gränser – om invandrarpolitiken
MOU 1999:1 För Sverige – på tiden!
MOU 1998:1 Samhällsmoral i praktiken
MOU 1997:1 Entreprenören i högsätet
MOU 1996:2 Kommunala företag – hot mot demokrati
MOU 1996:1 Den nya arbetsrätten – ett förslag
MOU 1995:3 Järntrianglar – förnyelsens fiende nummer ett
MOU 1995:2 Irrfärdens slut – för sunda statsfinanser
MOU 1995:1 När folkhemmets barn blivit vuxna
MOU 1994:1 HSF-modellen – patientmakt och kvalitet
MOU 1993:2 Charta Nova – politik för entreprenörskap
MOU 1993:1 Barnomsorg enligt kundvalsmodellen
MOU 1992:2 Hälso- och sjukvård för 2000-talet
MOU 1992:1 Eget val i äldreomsorgen – handledning
MOU 1991:6 Hur man säljer allmännyttehus – handledning
MOU 1991:5 På egna ben – reformera organisationsstödet
MOU 1991:4 Skolpeng hösten 92 – en handlingsplan
MOU 1991:3 Självständiga kommuner
MOU 1991:2 Sänkta skatter för en ny välfärd
MOU 1991:1 Företagsamhetens förutsättningar
MOU 1990:3 En marknad för bostäder åt alla
MOU 1990:2 Medborgarnas miljömanifest
MOU 1990:1 Minska statsskulden – sälj tillgångar
MOU 1989:1 Sänkt skatt för alla
MOU 1988:1 En ny grundlag – ett förslag

Facebooks grundare Mark Zuckerberg har sagt: ”Just get over it - no one cares about privacy anymore”. Glöm integriteten, alltså.

Samtidigt kan man konstatera att ju mer personliga detaljer som människor lägger ut om sig själva på Facebook, desto mer pengar tjänar företaget. Det beror på att annonserna på sajten kan riktas till en mera nischad målgrupp. Hösten 2011 släppte Facebook nya applikationer som gör att vännerna (och Facebook själva) sekund för sekund kan följa exakt vilken tidningsartikel du läser, vilket teveprogram du tittar på och vilken låt du lyssnar på. Det är bara ett exempel i raden på hur världens största sociala nätverk alltmer kryper under huden på sina medlemmar.

I USA är det redan vanligt att myndigheter blir ”vän” med medborgare vars ärenden de handlägger, för att kunna kontrollera dem bättre. Och i forskningslabben drivs projekt som exempelvis syftar till att programvaror automatiskt ska kartlägga människors personlighet baserat på vad de skriver och gör i sociala medier.

”Storebror på Facebook” redogör för övervakningsprojekten och påvisar riskerna för ett storebrorssamhälle, men ger också tips på hur man skyddar sin integritet i sociala medier, hur brottsligheten på Facebook ser ut, hur polisen arbetar på Facebook och vilka tankegångar som finns på lagstiftning och reglering av sociala medier.

Pär Ström är integritetsombudsman vid Den Nya Välfärden. Läs även hans fem tidigare rapporter om integritet. De kan laddas ned eller beställas från: www.dnv.se/podcast

den nya välfärden

Box 5625, 114 86 Stockholm | tel 08-545 038 10
www.dnv.se | integritetsombudsmannen@dnv.se