Vadå privatliv?

– Om det framväxande övervakningssamhället

PÄR STRÖM

Vadå privatliv?

– Om det framväxande övervakningssamhället

Pär Ström

www.dnv.se
Omslag: Vikman kommunikation, Vällingby
Layout och sättning: Desktop Ateljén AB, Finnerödja
Tryck: ÅD Tryck AB, Bromma, 2013
ISBN 978-91-977488-5-8

Innehåll

1. Introduktion

Människor lämnar efter sig ständigt ökande mängder elektroniska fotspår. Till exempel får vi allt fler vardagsapparater som är digitala och uppkopplade, vilket innebär att fotspår skapas och att vi kan övervakas.

Samtidigt utvecklas i rask takt nya verktyg för att analysera de elektroniska fotspåren och därmed kunna dra slutsatser om hur vi är och hur vi lever våra liv. Det kan röra sig om relationsanalys, personlighetsanalys, åsiktsanalys, automatisk ansiktsigenkänning på gator och torg och andra mer eller mindre orwellianska metoder. Det är symboliskt för utvecklingen att det var ett digitalt verktyg avsett för terrorbekämpning som användes av polisen för den olagliga registrering av romer som avslöjades nyligen.[1]

Denna bok inleds med ett scenario, ”Evas mardröm”, som visar hur de elektroniska fotspåren enkelt kan göra en människas liv till en fasa om det vill sig illa. Därefter utvecklar jag på ett antal sätt problematiken kring elektroniska fotspår och övervakningssamhällets framväxt.

Trots ivriga försäkringar från de politiska och kommersiella etablissemangen om att våra data är säkra måste man konstatera att den digitala världen kryllar av dataläckor. Även från de mest osannolika källor, även från de databaser man tror är allra mest skyddade. Sådan är verkligheten, och det visar jag exempel på i ett av bokens kapitel.

I ett annat kapitel tar jag upp tankar kring vilka integritetshot som ännu inte riktigt har materialiserat sig, men som lurar runt hörnet. Jag för också en diskussion om varför integritetsfrågan idag är så lågt prioriterad av människor och det politiska etablissemanget, trots att hotet är värre än någonsin. När en folkräkning skulle genomföras på 1980-talet var protesterna stora. Ändå var informationen som då samlades in ett spott i havet jämfört med vad som samlas in idag – utan att (särskilt många) människor bryr sig.

Avslutningsvis ger jag ett antal tips på åtgärder som en vanlig människa relativt enkelt kan vidta för att skydda sig mot intrång, digistalking, IT-baserade bedrägerier och andra former av IT-relaterade problem. En lista på skyddande programvaror och tjänster finns också.

En bok om övervakningssamhället som kommer ut hösten 2013 hade inte varit komplett om inte den amerikanska avlyssningsmyndigheten NSA:s massövervakning avhandlades. Man kan konstatera att NSA-spionaget skakar IT-samhället i sina grundvalar, en utveckling som vi bara har sett början av. När företag, myndigheter, politiker och privatpersoner fullt ut har hunnit ta till sig det faktum att det knappt finns en sladdstump som inte har öron uppstår viktiga problem. Detta behandlas i kapitlet ”Betydelsen av NSA:s spionage”.

Syftet med denna bok är att väcka liv i integritetsfrågan. Att få enskilda människor att engagera sig, att få politiker att prioritera integritetsfrågan och att få företag att respektera integriteten i sina produkter och tjänster. Allt måste starta underifrån, i en efterfrågan på personlig integritet. Om människor inte uppskattar och kämpar för bevarandet av privatlivets helgd kommer denna snart att vara ett minne blott.

Tidigare skrifter om integritet

Tidigare har jag skrivit nedanstående skrifter om personlig integritet och övervakningssamhället för Den Nya Välfärden. Samtliga finns för gratis nedladdning i pdf-version på Integritsombudsmannens sida på www.dnv.se. En del finns fortfarande kvar i pappersversion och kan beställas utan kostnad.

- Storebror på Facebook (2011)
- Storebror tar fram munkavlen (2009)
- Integritetens lilla röda (2008)
- Med storebror i byxfickan (2007)
- Med storebror i uppfinnarverkstan (2006)
- Med storebror i baksätet (2006)

Ett pdf-utdrag ur min bok ”Övervakad” från 2003, som behandlar amerikansk digital övervakning av andra länder, finns gratis tillgängligt på samma sida. Titeln är ”Amerikansk avlyssning från Echelon till Prism”.

Video- och podcastintervjuer

På Integritetsombudsmannens sida under www.dnv.se finns också ett antal video- och podcastintervjuer om personlig integritet som jag gjort med olika intressanta personer, till exempel Alexander Bard, Leif GW Persson och Annie Lööf.

Pär Ström
September 2013
par.strom@dnv.se

2. Evas mardröm

Överallt och ingenstans

I takt med att Eva gled över från drömmarnas värld till vaket tillstånd ökade hennes ångest. Hon kastade en blick på klockradion, som visade 05.12. Det var fortfarande mörkt, men en snabb handrörelse kunde bekräfta att maken låg där alldeles intill. Kurt. Det var egentligen självklart, men gjorde henne ändå en aning lugnare.

För hundrade gången gick hon för sitt inre igenom vilka fiender hon hade. Egentligen tyckte hon det var märkligt att hon över huvud taget skulle ha fiender – hon var ju en vanlig journalist med ett Svenssonliv. Men efter vad som hade hänt måste hon ju ha det.

Eva hade tre idéer om vem som kunde ligga bakom de skrämmande mejl hon fått de senaste veckorna. Den första tanken var hennes ex, som hade blivit väldigt aggressiv när hon gjorde slut. Det var visserligen fem år sedan, men Eva hade en obehaglig känsla när det gällde honom. Medan de var ihop hade han varit vansinnigt svartsjuk – det var faktiskt en viktig anledning till att hon lämnade honom. Han hade gång på gång snokat i hennes mobil, och på något sätt misstänkte hon att han hade lyckats ta sig in på hennes Hotmail-konto trots att hon aldrig lämnat ut lösenordet. Exet var IT-kunnig och jobbade som programmerare på ett stort IT-företag. Nörd.

För ett par månader sedan hade exet hört av sig till Eva och ville träffas. Hon hade dragit på svaret av rädsla för att reta upp honom, men till slut svarat nej. Sedan hade hon inte hört något.

Nästa tanke gick till den där hantverkaren som Eva hade anlitat för att renovera badrummet. Kakla, lägga klinker, sätta upp nya skåp och montera läckra LED-belysningar. Han hade inte gjort färdigt detaljerna, trots ihärdigt tjat från Eva, och dessutom hade hennes bror (som var i byggbranschen) upptäckt att underlaget var felaktigt utfört. Jobbet uppfyllde inte kraven för våtrum.

Hantverkaren hade skickat faktura, men Eva krävde naturligtvis att allt skulle fixas innan hon betalade. Då hade han gått i taket, börjat skrika i telefon och sagt att han minsann kände folk som kunde trycka på. Ja, så hade han sagt – ”trycka på”. Med ett otäckt tonfall.

Eva hade spontant fått associationer till Hells Angels-indrivning, men några motorcykelkillar hade inte dykt upp. Det hade däremot dessa hemska mejl. Men var det verkligen troligt att en våtrumshantverkare hade förmåga att dra igång en sådan långtgående digital kartläggning av hennes liv?

Hennes tredje tanke var nog den otäckaste. På redaktionen hade Eva varit huvudansvarig för ett grävande projekt där de undersökt korruption och svarta pengar i Stockholms restaurangbransch. Den ena tråden gav den andra, och efter ett tag hade Eva trängt så djupt in i problemet att det börjat kännas riktigt obehagligt. Hon hade insett att det var stora pengar på spel och därmed mäktiga krafter hon utmanade. Och personer som definitivt inte var några mysfarbröder.

Klockradion visade 05:39 när Eva steg upp den morgonen. Hon hade bara en kvarts resa till jobbet, men hon hade

kommit på att ångesten var som värst när hon låg overksam i sängen. Lika bra att stiga upp alltså.

Eva satte upp det långa mörkbruna håret i en hästsvans, tog på sig sin laxrosa morgonrock, gick ut i köket och fyllde vattenkokaren. När hon tryckte på startknappen tänkte hon på att den digitala och trådlöst uppkopplade elmätaren skickade iväg information om aktuell elförbrukning så ofta att det var tekniskt möjligt för personal på elbolaget att se hur dags människor i ett visst hushåll steg upp på morgonen. Och några forskare hade visst kunnat använda elförbrukningens variation för att analysera vilken film som visades på en teveapparat.

Visst var Eva medveten om att man är klart paranoid om man tänker så. Men sedan hennes helvete började hade hon ägnat mycket tid åt att läsa på om digitala metoder för övervakning och snokande, och då kunde man faktiskt inte bli annat än paranoid.

Alltihop hade börjat tre veckor och två dagar tidigare i form av ett mejl med avsändaren ”Oculus”. I mejlet stod:

Skärholmen 18.08, Jennifer 20.34, BBC News 20.43, Bondegatan 20.57. Oculus

Det var allt. Egentligen var det en märklig slump att Eva ens läste det, mot bakgrund av spamflödet, men nu gjorde hon det.

Mejlet hade legat i inboxen när Eva kom till jobbet på morgonen, och det var fyra saker som gjorde det så speciellt:

– Kvällen innan hade hon åkt tunnelbana till just Skärholmen, där hon stämt möte med sin bror kl 18. Men hon hade kommit fram något försenad...

– På vägen hem hade hon ringt sin dotter Jennifer, som numera bodde i USA. Det måste ha varit runt halv nio hon ringde det samtalet...

– Efter att ha pratat en liten stund med Jennifer hade Eva slösurfat med mobilen, och börjat med den engelska nyhetssajten BBC News...

– Eva hade kommit hem till lägenheten – som låg på Bondegatan – precis i tid för att hinna se sitt favoritprogram ”Efterlyst” på TV3. ”Efterlyst” börjar kl 21.00...

Creepy är bara förnamnet, hade Eva sagt till Kurt när hon ringde från jobbet och berättade det hela. Sedan dess hade det bara blivit värre. Mycket värre. ”Oculus” hörde nämligen av sig varje morgon. Så gott som prick klockan 8, och alltid med rapporter om vad Eva hade gjort dagen innan.

Och det stämde. In i minsta detalj.

Naturligtvis hade Eva kontaktat polisen. De tog mycket seriöst på det, och satte Eva i kontakt med en specialist på stalking. Men där tog det stopp. Polisen kunde inte göra något, sa de, och de hade ingen aning om hur Oculus fick sin information.

”Vet du att ‘Oculus’ är latin och betyder ‘öga’?”, hade stalkingexperten frågat. Det hade Eva inte vetat.

Hur kunde polistjejen veta det? Var hon insyltad i en konspiration? Tanken hade farit genom huvudet på Eva, innan hon insåg att hon måste se upp så hon inte blev tokig på riktigt.

Om Eva istället hade haft någon efter sig som skuggade henne på gammaldags vis så hade det varit otäckt nog, men ändå mycket bättre. En gubbe i trenchcoat och hatt som står och väntar under gatlyktan var ändå något påtagligt, något man kunde se, något man kunde skydda sig mot. Men det

som drabbat Eva var av en annan art – hennes skugga var överallt och ingenstans.

Magen värkte av oro medan hon hällde kokande vatten över den blå keramikmuggen med en påse Darjeeling-te. Hon var också lätt illamående. Eva tittade på sitt armbandsur för att se hur lång tid det var kvar till klockan 8. Hennes liv hade numera en daglig kulmen vid det klockslaget – en nervslitande, vidrig kulmen som successivt bröt ned henne.

För så kändes det. Eva höll på att gå under.

Samtidigt som Eva slog sig ned vid köksbordet hällde en annan person, på en annan plats, upp en kopp hett kaffe. Den personen bar en vinröd tröja av fleece. Kaffekoppen placerades på ett enkelt bord i ett litet rum som var ganska dunkelt eftersom en tjock mörkbrun gardin var fördragen.

Eva hällde en skvätt mjölk i tekoppen och tog en första klunk av sitt te, vilket numera var det enda hon konsumerade på morgnarna. Förr hade hon alltid ätit tre skivor rostad Pågens jättefranska med ost, helst Havarti, men sedan hennes inferno börjat hade matlusten försvunnit. Alldeles särskilt på morgonen. Och Havarti-ost ville hon nog aldrig mer äta, efter att Oculus i en rapport påpekat att hon köpte sådan.

Hur kunde han veta det? Vad visste han mer? Frågan gnagde sig allt djupare in i henne.

Inget ont som inte har något gott med sig – Eva hade gått ned tre kilo på dessa veckor. Men den här bantningsmetoden ville hon inte ens att hennes värsta fiende skulle drabbas av.

Fiende, där dök ordet upp igen. Vem kunde det vara? Eva slog bort tanken.

Hon tog ännu en klunk te.

Eva drog laddarsladden ur sin iPad och satte igång den. Knappade in ”dn”, varpå webbläsaren fyllde i resten och

strax hade hon Dagens Nyheters startsida framför sig. Hon klickade på en artikel om skuldkrisen i Europa – och funderade på om den skulle komma med i Oculus nästa rapport från hennes liv.

Eva hade blivit väldigt restriktiv med vilka artiklar hon läste, och inte bara det, utan över huvud taget med vad hon gjorde i den digitala världen. Vilka hon ringde och messade, vilken musik hon lyssnade på i Spotify, vilken film hon streamade på kvällen, och så vidare. Hon tänkte inför varje klick och varje digital handling på vilket intryck det kunde ge och hur det eventuellt skulle kunna misstolkas, förvrängas eller användas mot henne. Skuldkrisen borde väl vara rätt harmlös att läsa om?

En kväll, några dagar efter att helvetet börjat, hade Eva som en del av sin research om stalkingen googlat ”storebror ser dig metoder”. Dagen efter stod det ”storebror ser dig metoder, kl 17:13” i Oculus mejl. Och så var det en vidrig leende smiley efteråt. Det var enda gången Oculus visat prov på humor, eller över huvud taget någon slags känslorörelse. Sedan dess hade Eva använt DuckDuckGo inställt för Google – men hon visste inte om det gjorde någon skillnad.

Eva gick fram till fönstret, drog undan den skira ljusblå gardinen och tittade ned på gatan – något hon gjorde ofta nuförtiden. Naturligtvis helt förgäves. Inte en enda gång hade hon sett någon trenchcoatförsedd snok med hatt stå och röka under lyktstolpen, eller över huvud taget någon som skilde ut sig från alla stressade Svenssons. Hennes mardrömsskugga var digital – en digistalker. Men det hade ändå blivit rutin att se sig omkring, titta över axeln, hålla koll – för numera var Eva otrygg dygnet runt.

Samtidigt som Eva noga drog för gardinen igen klickade personen med vinröd tröja igång en applikation på sin dator. En stor ruta som såg ut som någon slags kontrollpanel dök upp på skärmen. Det rykte ur kaffekoppen.

För Eva kändes det som en evighet innan hon hörde att Kurt började vakna till liv. Hon gick mot sovrummet, men mötte sin man på vägen och de slog sig ned tillsammans vid köksbordet.

”Vad du ser blek ut”, sa Kurt.

Hon suckade. ”Har du hört av den där säkerhetsfirman?”

”Ja. Det gav inget.”

”Vad sa de då?”

”De skulle kunna gå igenom våra apparater, och det kostar skjortan för det första, men det är bara lokala grejer de kan hitta.”

”Lokala?”

”Ja, spår i själva apparaterna?”

”Och?”

”Nån verkar ju samla in data på andra ställen, och där har firman ingen befogenhet.”

Eva suckade igen. Kurt fortsatte:

”Och förresten verkar de inte nåt vidare pigga på att ha privatpersoner som kunder över huvudtaget”.

Eva satte armbågarna på bordet och begravde ansiktet i handflatorna. Hennes fingertoppar masserade nervöst de stängda ögonen. Kurt flyttade stolen närmare och la armen runt henne. Så satt de, under tystnad, en lång stund. Man kunde höra den mekaniska klockan i köksfönstret ticka – det var arvegods från Kurts farmor. Från den predigitala tiden.

Eva lyfte på huvudet.

”Tur att han inte har börjat förfölja dig i alla fall”, sa hon.

Kurt nickade. Tanken hade slagit honom, och han insåg att det kunde varit värre. Mycket värre.

Och det kunde det fortfarande bli.

Hittills hade Oculus bara intresserat sig för Eva. Inte för Kurt, och inte för Jennifer.

Eva reste sig upp.

”Jag går tidigt”, sa hon. ”Kan lika gärna sitta på jobbet”.

Kurt tänkte att hon såg gammal ut. Sliten. ”Du borde ringa läkaren”, sa han.

”Den triumfen vill jag inte han ska få.”

Kurt visste inte vad han skulle säga, så han förblev tyst. Men han hade i alla fall lyckats så ett tankefrö hos Eva, och hon grubblade länge på möjligheten att gå till läkaren. Kanske bli sjukskriven. Eller få ångestdämpande medicin. Men, insåg hon, då skulle Oculus få negativ information om henne för sitt arkiv.

‘Arkiv’ var det ord som makarna hade börjat använda om Oculus data. ”Vad ska han göra med arkivet, tror du?”, frågade Eva.

Kurt funderade i några sekunder.

”Förr eller senare får vi väl veta”.

Det gick en ilning genom magen på Eva. Plötsligt kändes det som om hon skulle kräkas, men det gick över.

Kurt hade lämnat tvätt i torkrummet kvällen innan, och Eva kilade ned för att hämta den. När hon höll fram nyckelkortet mot läsaren för att låsa upp tvättstugan kastade hon en blick på sitt armbandsur, och noterade tiden 06.37. Det var för att kunna kontrollera Oculus klockslag, om detta skulle dyka upp i hans nästa mejl.

Eva packade ihop de saker hon skulle ha med till jobbet. Bland annat boken ”Healingkoden: sex minuter för att läka

orsaken till dina problem", som skulle tillbaka till biblioteket. Hon funderade på att linda in boken i aluminiumfolie, med tanke på vad hon läst om att en främling med en antenn under jackan kunde läsa av bibliotekets lilla radiochip i boken om han kom tillräckligt nära. Metall skärmar av radiovågor. Eva kom dock fram till att boken inte var tillräckligt känslig för att motivera omaket, och förresten kändes det osannolikt att Oculus skulle sätta sig intill henne på tunnelbanan.

Det tog runt fem minuter att gå till stationen. Eva vände sig om flera gånger under promenaden dit, men såg inget onormalt. Solen sken och det var ljumt i luften, men det doftade avgaser. När Eva höll fram sitt kollektivtrafikkort i spärren tänkte hon än en gång 'märker han detta?'.

Hon var inte säker på om Oculus hade tillgång till kollektivtrafikens data om när och var människor använder sina Accesskort. Många gånger hade han lämnat information om hennes geografiska uppehållsort i sina mejl, men det var oklart om dessa baserade sig på kortavläsning i tunnelbana och bussar eller avläsning av mobilens position. Eller något annat. En gång hade Oculus kommenterat en bilfärd som Eva gjort så att hon fått intrycket att han hade tillgång till biltullarnas databas. Nu hade Eva stängt av den där appen som registrerade var hon befann sig och delade informationen med hennes vänner.

Samtidigt som Eva gick in i tunnelbanan tog personen i det dunkla rummet en klunk av det svarta kaffet, och greppade sedan musen. Markören gled långsamt fram över bildskärmen, stannade till en kort stund vid knappen "Hear surroundings", för att sedan glida vidare till "Website monitoring". Där hovrade markören i några sekunder, tvekande, för att sedan röra

sig till ”Track location”. Man hörde ett klick, och efter några sekunder dök det upp en karta upp med en blå prick i mitten.

När tunnelbanans strålkastare syntes i tunneln tänkte Eva att det nog var så här självmordskandidater kände sig. De stod på perrongen och tittade in i tunneln och tänkte att livet är ett helvete. Väntande. Tvekande. Eva ryste till.

Tåget närmade sig i hög fart och hon tog instinktivt ett steg bakåt. Några suicidala tankar hade hon inte, så långt hade det inte gått. Dock hade hon börjat fundera på vad som ligger bakom människors självmord, och hon hade fått en ny förståelse för dem som tar steget.

‘Ont krut förgås inte så lätt’, hade Evas farmor haft för vana att säga, sådär lite skämtsamt. Talesättet kändes just nu väldigt relevant för Eva. Hon måste härda ut.

Så lätt förgås inte ont krut! tänkte hon och steg in i tunnelbanevagnen. Farmor var en lyckans ost som fick leva sitt liv i det predigitala samhället. Inga elektroniska fotspår. Ingen Oculus.

Eva höll fram sitt passerkort för att komma in i tidningshuset, och tänkte den där tanken igen. Noterar han detta?

När hissen gick uppåt verkade fjärilarna i magen ha bestämt sig för att hålla flyguppvisning. Hon började andas häftigt och kände sig yr. När hissdörrarna gick upp störtade hon ut, missade att besvara hälsningen från Linus på marknadsavdelningen och sprang till sitt rum. Bara för att hinna sätta sig ned innan hon svimmade.

Morgnarna var mardrömmar numera, eftersom hela hennes kropp fasade för 8-slaget.

När Eva suttit på sin stol någon minut kändes det lite bättre. Inte med magen, den var ett upprört inferno, men

svimningstendensen hade gått över. Hon stängde det fönster hon tidigare vräkt upp för att få riktig luft.

Plötsligt stod Linus från marknadsavdelningen i dörren. Hans ljusgula lugg och klarblå tröja fick henne att tänka på seriefiguren 91:an Karlsson.

”Hur är det med dig, Eva?”, frågade Linus. Frånvaron av leende och sättet han sa det på vittnade om att det inte var någon artighetsfras.

En kort sekund övervägde Eva att tala ut.

”Jorå, det är bra”, hörde hon sig själv säga, och insåg att hon än en gång tackat nej till ett potentiellt stöd. Det var på slutet många som på olika sätt hade frågat henne hur det var. Men hon orkade inte sitta och berätta för sina arbetskamrater och känna sig dum och misslyckad.

Linus tvekade en sekund, drog sedan ett lite krystat leende över sina läppar och försvann.

Eva kom att tänka på det där reportaget från förskolan som hon hade lovat redaktionssekreteraren. Han hade påmint henne två gånger, och den andra gången anade hon en återhållen irritation i hans röst. Skärp dig Eva, du sitter löst! tänkte hon. Problemet var bara att ångesten låg som en våt filt över hela hennes existens, och både arbetskapacitet och kreativitet var nere på ett minimum.

Men hon visste hur arbetsmarknaden såg ut för journalister, så hon insåg att hon måste skärpa sig. Hon och Kurt hade ju stora lån på lägenheten, och marginalerna var minimala.

Det högg till i magen av oro.

Eva tänkte på sin kompis Åsa, som hon lärt känna på Journalisthögskolan. Åsa hade åkt ut från en konkurrerande tidning i en av branschens många neddragningar. Hon hade sedan letat jobb hela dagarna, men det var som att leta oxfilé

på en roslagsklippa. Hon kunde inte ens fixa något frilansuppdrag, trots att hon var både duktig och uppskattad. Nyligen hade Eva läst på Facebook att Åsa tagit ett städjobb.

Lyckans ost!

Ja, precis den tanken flög genom Evas huvud. Hon hade varit överlycklig om hon kunnat byta liv med Åsa.

När klockan var fem över åtta, och Eva tog tag i musen för att tömma sin e-post, var hon så nervös att den svettiga handen skakade. Magen var ett hav i storm och hon andades stötvis.

Efter en massa spam dök det upp, mejlet från Oculus, och Eva stålsatte sig. Långsamt, långsamt förde hon musen mot den vidriga raden. Hon var kallsvettig. Det var som en golgatavandring. Till slut kunde hon inte skjuta upp det längre utan dubbelklickade snabbt på rubriken.

Den här gången var det ingen text i mejlet, utan bara en bilagd fil. Den hade namnet ”klicka- här.mp3”. Eva dubbelklickade.

Det tog några sekunder, och sedan började det brusa svagt om datorns högtalare. Strax hördes en avlägsen mansröst som lite otydligt sa ” Hur är det med dig, Eva?”. Efter ytterligare några sekunder svarade en kvinna med starkare röst ”Jorå, det är bra”.

Eva satt som förstenad. Det här var ju hennes dialog med Linus tio minuter tidigare!

Yrseln kom över henne igen, och det kändes som om hon skulle svimma. Eva flög upp från stolen och la sig på golvet för att inte falla omkull och slå sig. Ångesten var våldsam och hon andades flåsande, ja hon hyperventilerade. Det började sticka i händer och fötter som om de hade somnat. Yrseln

blev allt värre. Jag håller på att dö, tänkte hon. Jag känner det. Infarkt. Det måste vara en infarkt.

Eva skrek på hjälp. Sedan kände hon hur kraften att ropa försvann. Rösten fungerade inte. Det gav panikkänslor. Hon flåsade våldsamt medan omvärlden försvann i dimmor.

Hennes nästa upplevelse var att någon höll en tratt över ansiktet på henne, och två personer i grönt böjde sig ned över henne. ”Andas normalt”, hörde hon en lugn och trygg manlig röst säga. Eva kunde inte röra på armar och ben, och de verkade vara fulla av tusen nålar. ”Andas normalt”. Hon blev medveten om att hon faktiskt flåsade och tvingade sig själv att följa uppmaningen. Den ena grönklädda ställde sig upp. ”Bra ansiktsfärg”, hörde hon honom säga. Eva koncentrerade sig på andningen: Andas in – vänta lite – andas ut. Inte för fort. Andas in – vänta lite – andas ut.

Världen började långsamt återvända. Eva tittade sig omkring och upptäckte att halva redaktionen stod i hennes rum och såg ut som om de var på begravning. Allas blickar var riktade på henne. Det kändes konstigt att se sina arbetskamrater underifrån. Fia hade en maska på strumpbyxorna inne under kjolen, noterade Eva, och plötsligt kändes hela situationen väldigt pinsam. Med stor möda inledde hon försök att sätta sig upp. Hon ville upp, upp, upp.

Ambulanspersonalen tog henne med till sjukhuset, men utan blåljus, för hon kände sig nästan lika stark som vanligt och kunde till och med själv knäppa spännet på bårens bälte. Efter att ha tillbringat halva dagen med att genomgå diverse undersökningar, inklusive skiktröntgen av huvudet för att upptäcka eventuella tecken på stroke, fick hon komma in till en läkare för besked.

De fula landstingspersiennerna i fönstret var neddragna men vinklade öppna, och Eva kisade i motljuset.

”Det är inget fel på dig”, sa doktorn, en lätt överviktig kvinna i övre medelåldern med vit rock och en rödaktig pagefrisyr. ”Fysiskt”.

Det där sista ordet tog som en pil. Eva förstod naturligtvis vad läkaren insinuerade, och hon tittade ned.

Vitrocken satte huvudet på sned, tittade underligt på Eva och frågade:

”Hur mår du – EGENTLIGEN?”

Hon visste inte vad hon skulle säga, hon bara satt där och tittade på doktorn. Så, plötsligt, släppte alla hämningar. Eva började gråta våldsamt. Kroppen skakade och tårarna flödade. Läkaren höll om henne, lite tafatt, men det hjälpte inte. Eva grät bara ännu mer.

Och hon kunde inte sluta.

Efter en stund tog läkaren upp den trådlösa telefonen ur fickan och ringde ett samtal, och snart kom en sköterska med en säng. Eva fick en gul landstingsfilt över sig och rullades iväg. Hennes gråt började avta, och snart upphörde den – det fanns ingen kraft kvar. Istället började hon tänka, men det var knappast något steg framåt.

Sköterskan svängde med sängen från en korridor in i nästa då Eva råkade se en övervakningskamera på väggen. Snabbt drog hon upp filten över ansiktet. Hon var rädd för Oculus.

Eva hamnade i ett enkelrum, och knappt hade hon blivit lämnad ensam förrän hon somnade. Och där sov hon i flera timmar. När hon till slut vaknade var Kurts ansikte det första hon såg. Han log stort mot henne.

”Älskling, hur är det med dig?”

Eva log svagt. ”Jotack”, sa hon. ”Bättre nu. Vet inte vad som hände”.

Kurt tog Evas hand. ”Vi ska ta oss igenom det här, tillsammans”, sa han. ”Det ska vi!”. Eva kramade hans hand hårt och log stort.

En sköterska kom in i rummet, och hon sken upp när hon såg att Eva hade vaknat. ”Vad bra, då ber jag doktorn komma strax”, sa sköterskan och gick.

Den här gången var det en annan läkare, en mager man i 60-årsåldern med ett jovialiskt sätt.

Han satte sig intill sängen på en rund sjukhuspall av blank metall med hål i.

”Det är inget fel på dig, egentligen”, sa han till Eva. ”Du är utarbetad helt enkelt. Jag rekommenderar en riktigt lång och härlig semester!”.

Läkaren erbjöd Eva att stanna en natt på sjukhuset, men efter att ha konfererat med Kurt tackade hon nej. Eva satte sig långsamt upp i sängen. Kurt erbjöd sig att stödja henne, men hon klarade sig själv sa hon. De gick mot sjukhusentrén med avsikt att ta en av de taxibilar som väntade utanför.

När paret kommit in i baksätet såg Kurt lite konstig ut. ”Du Eva...”, började han. Aningen spänd berättade han så för henne att medan hon sov hade han ringt chefredaktören på tidningen där hon jobbade och skällt ut honom. Ja, Kurt använde de orden. Han hade anklagat tidningen för att cyniskt spela med en anställds liv och hälsa bara för att få fram en bra story, utan att ens ställa upp med hjälp när det gick snett. Chefredaktören hade tagit det på stort allvar. Samtalet slutade med att ett möte bokades in med Eva, Kurt och chefredaktören klockan 16 samma dag. Då skulle det även finnas en teknisk expert från ett IT-säkerhetsföretag närvarande –

tidningen skulle bekosta en utredning för att gå till botten med digistalkingen.

Eva blev lättad av att höra detta, samtidigt som hon inte visste hur hon skulle orka med mötet. Men efter att hon och Kurt suttit ett par timmar på ett riktigt fint café, där de åt napoleonbakelser och drömde om olika semestermål, kände hon sig mogen att ta tjuren vid hornen.

Några minuter efter klockan fyra visades Eva och Kurt in i tidningens styrelserum. Chefredaktören satt redan där tillsammans med två andra män, alla tre gravallvarliga. En av de okända männen, en ovanligt lång lintott i 30-årsåldern, gick genast fram till Eva och tecknade åt henne att lämna över mobilen. Något förvånad gav hon den till honom, varpå mannen tog bort baksidan och plockade ut batteriet. Eva fick tillbaka delarna.

Det visade sig att lintotten var teknisk expert från ett företag specialiserat på det som kallas computer forensics, alltså att finna spår efter brottslighet i digitala system. Den andra, en mogen gentleman i brun blazer, var privatdetektiv.

Ja, just det, privatdetektiv. Eva och Kurt tittade på varandra och log i smyg när de hörde denna titel. I deras föreställningsvärld fanns den yrkeskåren bara på film.

Tidningens chefredaktör var riktigt spak. Han var förfärad över vad som hänt Eva och lovade all hjälp, både med den tekniska utredningen och Evas hälsotillstånd. Kanske var han rädd för att Eva skulle gå till facket eller på annat sätt orsaka skandal.

Lintotten frågade ut Eva om hennes användning av IT-resurser, medan deckaren frågade ut henne om hennes relation till olika människor som hon hade haft kontakt med.

Han ställde också frågor om Kurts bekantskapskrets. Båda män gjorde anteckningar.

När mötet närmade sig sitt slut bad den tekniska experten att få med sig Evas dator och mobiltelefon. ”För analys på labbet”, sa han. Eva lät blicken gå mellan experten och Kurt, vilket chefredaktören uppenbarligen såg.

”Nu tar du två veckor tjänstledigt med full lön”, sa han med pondus och log. ”Var nu offline och off-the-radar ett tag. Det behöver du”.

Även om Eva först var lätt förfärad över tanken på att inte vara elektroniskt nåbar insåg hon ganska snabbt, efter mild påverkan från Kurt, att hennes chef hade rätt. En stor fördel var för övrigt att hon garanterat inte skulle drabbas av några mejl från Oculus så länge hon var offline.

Även deckaren fick med sig material när de skildes åt. I hans fall var det en lång lista med namn och fakta om personerna. Det var en stor del av både Evas och Kurts vänkrets och släkt, inklusive en del personer de inte hade haft någon kontakt med på ett decennium.

”Vi grejar det här!”, sa den tekniska experten när han skakade hand med Eva. Deckaren log och nickade instämmande. Tillsammans med deras självsäkra utstrålning ingav uttalandet Eva ett visst lugn.

Kurt lyckades ordna en veckas semester från sitt jobb efter att ha berättat om Evas kollaps, och redan dagen efter reste paret iväg på en sista-minuten-resa till Kreta. Faktum är att Kurt följde Evas exempel avseende digital frånvaro, och lämnade dator, iPad och mobil hemma. Hans chef knorrade, men Kurt var obeveklig. Han och Eva var alltså kommunikationsmässigt förflyttade tillbaka till 1980-talet – och efter den initiala abstinensen visade det sig att de älskade det! De

blev inte störda ideligen, som de var vana vid, utan kunde fördjupa sig i sin relation och njuta av mat, vin, vågor och vind. Hand i hand gick de längs stränder och genom små byar, som var helt underbara med undantag för de undernärda vildkatterna. Båda två var djurvänner och det skar i själen att se hur dessa djur led.

På den femte dagen låg det ett meddelande till Eva i hotellets reception. ”Ring mig”, stod det bara, följt av ett namn som Eva kände igen som deckarens. Det var som ett telegram man sett i gamla filmer, tänkte Eva – det fattades bara ordet ”stop”.

Naturligtvis var hon nervös så hon skakade. Kurt följde med Eva in på hotellets kontor, där de fick låna en sådan där gammaldags telefon som sitter fast i väggen med en sladd. Svart.

”Vill du att jag ringer åt dig?”, frågade Kurt. Eva, fullt sysselsatt med att bita på naglarna, nickade.

”Jag går ut”, sa hon.

”Är du säker?”

”Ja jag väntar där ute”, sa hon och gick.

Kurt tog luren och slog numret.

När han knappt tio minuter senare kom ut i lobbyn fann han Eva sitta i en av fåtöljerna med ett glas whisky i handen. Hon såg ut som om hon väntade på ett dödsbud. Kurt gick fram under tystnad, slog sig ned intill henne och tittade henne i ögonen.

”Det är löst”, sa han högtidligt.

Eva andades häftigt. ”Är det löst? Vem var det?”

Kurt drog på det innan han till slut sa: ”Anna”.

Eva höll på att spilla ut sin whisky på den vita klänningen. ”Var det Anna???”, sa hon högt.

”Ja Anna”.

Hon tittade ned i sitt glas med en blandning av förvåning och lättnad över ansiktet. Anna var Kurts före detta fru. Visserligen visste Eva att Anna varit svartsjuk på henne när hon blivit ihop med Kurt, men det var flera år sedan. Och då hade Kurt och Anna redan separerat. Eva hade inte kunnat drömma om att taggen satt så djupt – och att mänskan uppenbarligen var psykiskt sjuk.

”Spåren ledde till henne, deckaren åkte dit och hon erkände på en gång. Är väldigt ångerfull nu. Du får bestämma om du vill polisanmäla eller inte. Deckaren säger att han inte tror att Anna någonsin ställer till med problem igen.”

Eva bara stirrade framför sig. ”Herregud”, sa hon, och fortsatte stirra. Sedan svepte hon resten av whiskyn.

Eva satte ned glaset på det lilla soffbordet och tittade på Kurt. ”Men hur fick hon reda på allt om mig?”, frågade hon.

”Det var en spionprogramvara på din mobil. Allt kom från den. Så det där andra vi pratade om, biltullar och tunnelbana och bredbandsbolag och sånt, det var aldrig inblandat.”

Allt bara snurrade för Eva. Hon tittade ned. Tänk att det var Anna! De hade ju faktiskt setts på en fest några månader tidigare. Då hade de till och med pratat en stund, och Anna hade verkat ganska normal.

Plötsligt lyfte Eva blicken och tittade intensivt på Kurt. ”Nu kommer jag ihåg. Hon bad att få låna min mobil för hennes hade laddat ur. Och så var hon borta en stund...”

”A-ha”, sa Kurt, högt och utdraget, och såg ut som om han hade funnit Ljuset.

Det blev ingen polisanmälan, för Eva tyckte att Annas psykiska ohälsa var straff nog. Och det kom aldrig mer något mejl från Oculus. Det mesta återgick till vardagen för Eva och Kurt.

Men på en punkt blev det aldrig som förr. Paret kunde inte glömma hur underbart det varit att befinna sig off-the-radar, så fortsättningsvis blev det varje år en veckas semester utan en enda elektronisk pryl i bagaget!

Efterord

I det här scenariot hade Eva bara en vanlig ”Svensson” efter sig. Inte en teknisk expert, inte en insider anställd vid någon stor databas, inte någon från den organiserade brottsligheten med mycket pengar och stora resurser. Ändå blev hon så övervakad och avklädd som hon blev. Hade Evas digistalker varit en annan person – mera kunnig, mäktig eller välplacerad – hade den personen kunnat få fram ännu mer detaljer om Eva och hennes liv. Hur det skulle kunna gå till, och hur dataläckor har gått till i verkligheten, beskrivs i de följande kapitlen. Där finns också tips på hur man skyddar sig. För övrigt, om du vill se kraften i spionprogramvaror för mobiltelefoner kan du till exempel ta dig en titt på produkterna FlexiSpy[2] och Mobile Spy[3]. För övrigt avslöjades det i september 2013 att den amerikanska avlyssningsmyndigheten NSA har en bakdörr in i de flesta mobiltelefoner, bland annat iPhone och Android-baserade telefoner.[4]

Nästa kapitel har viss karaktär av lista, eftersom jag där går igenom vilka elektroniska fotspår som uppstår och var. Därefter kommer flera kapitel som är av resonerande karaktär.

3. Hur kan kartläggningen av Eva ske?

Det beskrivna scenariot Evas mardröm är tekniskt möjligt redan idag. Det hade som sagt kunnat bli mycket värre om Evas stalker till exempel hade varit en hackare eller en anställd vid ett företag eller en myndighet med en stor databas.

I detta kapitel listas ett antal exempel på elektroniska fotspår i vardagen och hur/var de uppstår. Jag har valt att organisera framställningen efter typ av information istället för efter apparat/teknologi, eftersom det ju är informationsslaget som avgör hur en människa kan påverkas. Några källor till data är dock generella och kan ge många typer av information, och för att undvika upprepningar nämns dessa inledningsvis separat. Se även avsnittet ”Några specialfall” sist i detta kapitel, även dessa av generell karaktär.

Generella källor

Spionprogram. Den som lyckats få in ett spionprogram i en människas dator eller mobiltelefon har möjlighet att komma åt allt. Alla filer kan läsas, e-post och chatt kan läsas, surfande kan övervakas och så vidare (gäller det en mobiltelefon kan även geografisk position övervakas). Därför kan i stort sett alla typer av information som behandlas i detta kapitel inhämtas

av den som kontrollerar spionprogrammet. Ett sådant kan till och med avlyssna rummet och titta in i det (om webbkamera finns).

Internetleverantören/teleoperatören. Av tekniska skäl kan internetleverantören se vilka sajter deras kunder besöker och vad de gör på sajterna, vilket i förlängningen ger möjlighet att inhämta många av de informationsslag som nämns i detta kapitel. Om man ansluter till en webbplats med https- protokollet (istället för http) är förbindelsen dock krypterad, vilket medför att internetleverantören bara kan se vilken sajt som besöks och inte vad som uträttas där. Internetleverantören har också tekniska förutsättningar att läsa e-post och chatt, vilket exempelvis avslöjar vänkretsen men också mycket annat.

Trådlösa nätverk. Om du kopplar upp dig mot någon annans trådlösa nätverk, exempelvis i ett köpcentrum eller en restaurang, får nätverksägaren samma tekniska förutsättningar för avlyssning som ovan beskrivs för internetleverantören. Om nätverket inte är krypterat kan dessutom andra personer som befinner sig i närheten av nätverket ta del av vad du gör och eventuellt, om de vill, styra om trafik som inte är krypterad. Den som kopplar upp sig har också lämnat ifrån sig det geografiska fotspåret ”jag var här”.

Var du befinner dig

En modern människa lämnar på många sätt efter sig elektroniska fotspår som röjer hennes geografiska position, alltså latitud och longitud på jordklotet. En del källor lämnar kontinuerlig positionsinformation, andra bara vid passage av vissa

datainsamlingspunkter eller i vissa situationer. Här följer ett antal källor till geografiska data om människor:

Mobiltelefonen. Mobiler kan på flera sätt användas av obehöriga för att kartlägga människors geografiska position och förflyttningar. Bland annat har de flesta mobiler GPS-mottagare, men även andra positioneringsmöjligheter finns.

Teleoperatörer. Ett mobilnät skulle inte fungera om inte teleoperatörerna varje sekund kände till var varje mobil befinner sig. Samtal och datatrafik ska ju kopplas via den närmaste antennmasten. Genom att samtidigt känna av en mobils signalstyrka från flera master kan teleoperatören få fram en noggrannare geografisk position än bara vilken mast som är närmast (detta kallas triangulering).

Enligt EU:s datalagringsdirektiv måste teleoperatörerna långtidslagra vissa data om sina kunder, bland annat mobiltelefoners geografiska position när de används.

Appar. De flesta människor har mängder av appar installerade på sin mobil, och dålig koll på vad dessa gör. En del appar sänder över geografisk position till appens utgivare, vanligen baserat på den inbyggda GPS-mottagaren. Detta ska visserligen godkännas av mobilens ägare då appen installeras, men många gör sådant slentrianmässigt. Dessutom har det vid upprepade tillfällen visat sig att appar inte sällan läcker och gör saker de inte skulle göra. Ett specialfall av appar är spionprogram – med ett sådant kan den som kontrollerar programmet följa telefonägarens rörelser.

Kollektivtrafik. Kollektivtrafikföretagen lagrar vanligen information om plats, tidpunkt och kortets nummer varje gång ett resekort används för att påbörja en resa. Man kan vara anonym, men många väljer att registrera namn och personnummer för att få förlustgaranti och andra fördelar. Ifall resekortets har laddats med hjälp av ett betal- eller kreditkort finns en identifierande koppling även om kortägaren inte registrerar sitt namn. Vid brottsutredningar har polisen möjlighet att få ut data från kollektivtrafikens register över resor.

Biltullar. Varje gång en bil passerar en av Stockholms eller Göteborgs sammanlagt 54 biltullar lagras information om registreringsnummer, klockslag och vilken plats det handlar om. I en rapport[5] har Trafikverket skrivit om användning av data från biltullarna för ”identifiering av unika fordon för analys av resmönster och restider”. Regeringen har beslutat att polisen i vissa fall ska få tillgång till data från biltullarna för brottsutredningar.[6] Motsvarigheter till biltullar finns vid vissa broar.

Restidssystem. I Stockholm, Göteborg och Malmö finns system med automatisk inläsning av bilars registreringsnummer i syfte att mäta restider. Dessa kallas restidssystem.[7] Kamerorna sitter ofta vid viktiga gatukorsningar och trafikknutpunkter, alltså vid andra platser än biltullarna.

Biltjänster. Det förekommer kommersiella digitala tjänster för bilister som bygger på att bilens geografiska position (GPS-baserad) överförs till tjänsteföretaget.

GPS-baserad vägskatt. På flera håll förekommer det, eller har förekommit, debatt om införande av GPS-baserad vägskatt. Det innebär att fordonsägaren beskattas efter var och hur mycket han/hon kör. Myndigheterna får alltså tillgång till den informationen. Detta har bland annat diskuterats i Nederländerna[8] och den amerikanska delstaten Oregon.[9]

Övervakningsförsäkring. Utomlands förekommer bilförsäkringar som bygger på att bilens geografiska position (GPS-baserad), hastighet och klockslag överförs till försäkringsbolaget via mobiltelefonnätet. I Sverige har Folksam fått Datainspektionens acceptans för att introducera en sådan försäkring.[10] Syftet är att kunna erbjuda kunderna rörliga försäkringspremier (att betala efter tagen risk).

Bilnavigatorer. De GPS-navigatorer som sitter i allt fler bilar lagrar genomförda resor där apparaten har använts.

Fartkameror. Sveriges 1077 fast monterade fartkameror har idag inte automatisk inläsning av nummerplåtar på alla passerande fordon (vilket skulle innebära registrering av geografisk position). Dock rapporterade media 2011 om funderingar från polisens sida på att införa just detta.[11] I Storbritannien finns ett mycket omfattande system av kameror i städer och längs landsvägar som automatiskt läser in alla passerande bilars nummerplåtar och lagrar informationen i två år.

Inköp. Varje gång ett konto- eller lojalitetskort används i en butik, restaurang, ett parkeringshus eller på annat ställe har innehavaren lämnat ifrån sig sitt digitala fotspår, vilket innebär geografisk positionering.

Bankomater. Samma sak gäller användning av bankomater.

Passerkort och digitala nycklar. Varje gång ett kort används som nyckel lagras passagen, och därmed innehavarens geografiska position vid det aktuella klockslaget. Inpasseringssystem är mycket vanliga på arbetsplatser, men börjar förekomma även i bostadshus och krävs då ofta även för åtkomst till biutrymmen såsom tvättstuga och vindskontor. Datainspektionens granskning har visat att flera bostadsföretag och bostadsrättsföreningar brister i sin behandling av de personuppgifter som uppstår i de digitala låsens loggfiler.[12]

Andra kort. Så snart ett personligt kort används för någon slags digital avläsning kan man utgå ifrån att geografiska fotspår uppstår. Ett exempel ur mängden är de system för att låna cyklar som finns i vissa städer, till exempel ”Stockholm City Bikes”.

Facebook. Den stora sociala sajten Facebook driver omfattande kartläggning av vad deras medlemmar gör med sin dator eller mobil. En analys har visat att användarens geografiska position är en av de saker som efterfrågas mest, och därför används som underlag för riktad annonsering.[13] En grov geografisk positionering går att göra via internet, utan användning av GPS-data eller inblandning av någon mobiltelefon.

Positioneringstjänster. Den som ansluter sig till en positioneringstjänst för att andra ska kunna se var man befinner sig (och vice versa) blir naturligtvis positionerad. Exempel på sådana tjänster är Google Latitude och den svenska tjänsten LociLoci.

Besökta sajter

Eftersom många slutsatser kan dras om en människa baserat på vilka sajter hon över tid brukar besöka är sådan information känslig. Vissa sajtbesök kan vara av mycket känslig karaktär. Information om människors surfande finns lagrad på många ställen och skulle kunna läcka på olika sätt. Här följer de viktigaste (utöver de generella som redan nämnts):

Appar. Det finns många appar som rapporterar till sin utgivare vilka webbplatser som besöks med den aktuella mobiltelefonen.

Facebook. Den som klickar på länkar till webbplatser inifrån Facebook lämnar efter sig information om det i Facebooks databas. Även om man är utloggad spårar Facebook i viss utsträckning surfandet – närmare bestämt registreras besök på de sajter som på något sätt är kopplade till Facebook (exempelvis genom att ha en gilla-knapp). Enligt den amerikanska tidskriften Business Insider har Facebook mer än 200 metoder för att spåra vad Facebook- användarna gör på internet (och då avses surfande som sker utanför Facebook).[14] En kvinna som använde sin rätt att begära registerutdrag om sig själv från Facebook fick en rapport på 880 sidor.[15]

Twitter. Så länge man är inloggad på Twitter registreras alla besök som görs på sajter som har en Tweet-knapp (en knapp för att skriva Twitter-inlägg).

Google. Den som surfar med Googles webbläsare Chrome och är inloggad hos Google lämnar efter sig hela sin surfhistorik hos Google. Ett annat exempel: I början av 2012 avslöjade

tidningen Wall Street Journal[16] att Google och en del andra annonseringsföretag hade åsidosatt de integritetsinställningar som människor gjort på sina iPhones, i syftet att spåra deras surfande. Detta åstadkoms genom en programvarukod som lurade webbläsaren Safari. Google kan också övervaka surfares aktivitet via Google Analytics, en tjänst som många sajtägare använder för att få statistik om hur besökarna rör sig på sajten.

Annonsnätverk. De stora nätverk som placerar ut annonser på en mängd olika webbplatser registrerar människors surfande med hjälp av exempelvis cookies. Därmed bygger de upp en allt större kännedom om varje surfares intressen och vanor, något som används för att kunna visa personligt anpassade annonser. Metodiken kallas ”behavioral targeting”. I de flesta fall har annonsnätverken från början inte kännedom om människors identitet, bara anonyma profiler, men den anonymiteten är ganska bräcklig. Exempelvis gör besök på sociala sajter ofta att det blir möjligt att sätta namn på profilerna. Nya teknologier som supercookies och digital fingerprinting gör det svårt för användarna att sätta stopp för annonsnätverkens spårning, det räcker inte längre att radera cookies.[17]

Webbplatserna själva. Det finns många knep för ägare till webbplatser att lägga samman två och två för att få kännedom om vilka som besöker deras sajt. Webbläsare lämnar ofta efter sig ett ”fingeravtryck” som är unikt. Du kan testa uniciteten hos din egen webbläsare med hjälp av en tjänst som tillhandahålls av medborgarrättsorganisationen Electronic Frontier Foundation.[18]

E-post, sms och ringande

Information om vem man ringer, mejlar och sms:ar avslöjar förstås vilka vänner man har, men den kan avslöja mycket mer än så. Det kan exempelvis röra sig om sjukdomar, politiska preferenser och andra åsikter. Innehållet i meddelandena säger förstås ännu mer. Denna typ av information kan finnas hos dessa aktörer (utöver de tidigare nämnda generella):

Globala internetföretag. Internationella jättar som Google, Yahoo, Microsoft, Apple och Facebook har naturligtvis tillgång till sina kunders e-postmeddelanden, sms-substitut, direktmeddelanden liksom andra meddelanden som de hanterar, vad än de kallas.

Arbetsgivare. Självklart har arbetsgivare möjlighet att ta del av e-post som går till och från sina anställdas konton. De har också teknisk möjlighet att ta del av privat e-post som anställda skickar eller tar emot via exempelvis Gmail eller Hotmail, om det sker från arbetsgivarens dator.

Skype. Vilken tillgång har Skype till sina kunders ringande och sändande av meddelanden? Kan de till exempel avlyssna samtalen? Frågan väcktes i början av 2013 av 45 medborgarrättsgrupper, som i ett brev till Skypes ägare Microsoft begär besked.[19] Klart är i alla fall att vissa länkar som Skype-användare skriver i sina chattmeddelanden överförs till Microsoft.[20] Efter Edward Snowdens avslöjanden måste man utgå från att NSA har tillgång till Skype-konversationer (liksom till det mesta på nätet).

Vad människor köper

Det är knappast känsligt om det kommer ut att en människa köpt en påse potatis, men det finns många andra inköp som kan vara av känslig karaktär. Här följer exempel på hur information om inköp samlas in, lagras och skulle kunna avlyssnas.

Surfande. Den som skaffar sig tillgång till en människas surfande får också kännedom om vilka varor hon köper i e-butiker. Se avsnittet ”Besökta sajter” ovan.

Bonuskort i butiker. Den som drar sitt bonuskort i kassan ger butikskedjan möjlighet att spara identifierad information om inköpen i databasen.

Kortbetalning. Även om det är ett steg omständligare har butiken teknisk möjlighet att koppla ett inköp till en viss person om personen betalar med kort, även om något bonuskort inte dras.

E-handel. Köper man på nätet är det närmast en självklarhet att e-butiken lagrar information om dina inköp. De lagrar vanligtvis också data om vilka varor du har tittat på, samt i övrigt vad du har gjort på deras sajt.

Kortföretag. Kortföretagen har förstås tillgång till information om varje gång kortet används: Inköpsställe, tidpunkt och belopp. Dock inte exakt vad som köptes. Handlar man i en stormarknad kan kortföretaget dra få eller inga slutsatser om vad man köpt, men handlar man i en specialbutik är situationen en annan. Den som handlat i ”Asiatiska matmarknaden” har förmodligen köpt asiatisk mat.

Facebook. Ett samarbete med datainsamlare ger Facebook tillgång till viss information om människors inköp, inte bara på webben utan även inköp gjorda i fysiska butiker (åtminstone gäller detta i USA).[21]

Vad människor läser

En människas läsande av artiklar, tidskrifter och böcker kan ibland säga väldigt mycket om henne. Det kan röra sig om åsikter, värderingar, intressen och planer. Här följer exempel på hur elektroniska fotspår om människors läsande kan uppstå.

Surfande. En människas surfande säger oftast mycket om vad han eller hon läser (se ”Besökta sajter”).

Facebook. Facebook har som nämnts ett stort intresse av information om vad användarna läser. De lagrar data om vilka länkar deras användare klickar på. Mer om detta finner du i min skrift ”Storebror på Facebook”, som finns kostnadsfritt tillgänglig på nätet som pdf.

Boklådor. Köper man en viss bok i en fysisk bokhandel eller internetbokhandel, och gör det på ett identifierande sätt, lämnar man naturligtvis fotspår efter sig. Den informationen gör att det kan betraktas som sannolikt att du läser den aktuella boken (men det kan förstås vara en present).

E-böcker. Den som läser e-böcker på en särskild e-boksplatta löper risken att utsätta sig för snokande. Det finns många läsplattor och de fungerar olika, men i varierande utsträckning förekommer både registrering av vilka boksökningar en

användare gör och vilka böcker han/hon verkligen läser. I en del fall registreras till och med vilka understrykningar läsaren gör under läsningen. Många e-boksrelaterade företag delar med sig av insamlade data till andra företag. Den amerikanska medborgarrättsorganisationen Electronic Frontier Foundation har gjort en ambitiös sammanställning av hur nyfikna de olika läsplattorna är.[22]

Bibliotekslån. Bibliotek lagrar naturligtvis människors lån i sina datasystem. Via hackning eller korrupt personal skulle den informationen kunna hamna i orätta händer.

Radioetiketter. Många bibliotek har numera satt radioetiketter (RFID) i sina böcker. Under vissa omständigheter kan det vara möjligt för en tekniskt avancerad person att med hjälp av en antenn läsa av radioetiketterna (om han eller hon lyckas komma nära, exempelvis på bussen) och därmed få information om vilka biblioteksböcker en annan person har i sin väska. Det kan till och med räcka med en mobiltelefon för att göra en obehörig avläsning av RFID-chip.[23] Dock krävs i de flesta fall tillgång även till bibliotekets databas, där bokens nummer matchas mot dess titel.

Musiklyssnande och tevetittande

Förr hade ingen annan människa någon aning om vilken musik du tyckte om, i alla fall inte efter att du hade stoppat ned den nyinköpta LP-skivan i påsen i affären. På samma sätt var tevetittandet av helt privat karaktär. När både musik och teve nu har digitaliserats är situationen en annan. Här följer

ett antal aktörer/metoder som skulle kunna sprida kännedom om ditt musiklyssnande och tevetittande.

Spotify. Om du använder Spotify för att lyssna på musik har de naturligtvis data om dina spellistor och val av låtar/artister.

Facebook. Om du använder både Spotify och Facebook informeras dina Facebook-vänner om vilka låtar du lyssnar på, såvida inte den funktionen stängs av. Då har dock Facebook själva ändå tillgång till ditt musikval.

iTunes. Köper du musik från Apples tjänst iTunes har naturligtvis Apple tillgång till ditt val av låtar/artister.

Teve: I många fall kan leverantören av tevekanaler via digitalboxen se exakt vilka teveprogram man tittar på i ett visst hushåll vid en viss tidpunkt.

Streamad film. Företag som streamar film till hushåll kan ha möjlighet att se vilka program/ filmer ett visst hushåll tittar på.

Elmätare. Två forskare kunde i ett forskningsprojekt använda mätdata från en elmätare för att analysera vilken film som visades på en teveapparat.[24] Det hela bygger på att en teveapparats momentana elförbrukning beror på hur ljus bild som visas, och ljushetens variation som funktion av tiden är unik för varje film.

Umgänge och vänkrets

Vilka vänner man har och vilka man i övrigt umgås med är information av mycket privat karaktär. Här följer ett antal sätt på vilka den informationen idag lagras digitalt eller/ och skulle kunna avlyssnas (utöver de inledningsvis nämnda generella sätten):

Mobilen. En mobiltelefon är en guldgruva för den som är intresserad av att kartlägga en persons vänkrets och umgänge. Adressbok och loggen över tidigare kontakter via telefon, sms eller e-post utgör mycket goda källor. Via elaka eller läckande appar, liksom via spionprogramvaror, kan informationen komma i orätta händer. För några år sedan lyckades ett säkerhetsföretag i USA bygga ett så kallat Bluetooth-gevär som kunde avläsa en mobiltelefons adressbok på 1.600 meters avstånd (utan spionprogram eller app).[25]

Avlyssning av dator. Via spionprogramvaror eller användning av icke-krypterade trådlösa nätverk kan obehöriga komma åt adressbok och annan detaljerad information om umgänge och vänkrets.

Sociala nätverk, särskilt Facebook, har information om sina användare som möjliggör en mycket långtgående kartläggning av deras umgänge och vänkrets.

Trafikdatalagring. Det av EU beslutade Datalagringsdirektivet innebär att teleoperatörer/ internetleverantörer åläggs att lagra så kallade trafikdata från sina kunders trafik, vilket inkluderar information om vilka personer som har haft kon-

takt via telefon, e-post eller sms. Detta utgör ett mycket bra underlag för vänkretskartläggning.

Webbmejl. Globala internetföretag såsom Google, Microsoft och Yahoo har möjlighet att kartlägga sina användares umgänge om dessa använder företagens respektive e-posttjänst.

Åsikter och värderingar

Genom att följa en människas digitala liv går det ofta att dra slutsatser om hennes åsikter och värderingar. Det kan bland annat ske på dessa vis:

Via surfande. Valet av sajter säger ofta mycket om vilka åsikter och värderingar en människa har. Se ”Besökta sajter”.

Via läsande. Digitalt läsande kan ske på annat sätt än genom att surfa, och är många gånger avslöjande för människors åsikter och värderingar. Se ”Vad människor läser” ovan.

Via Facebook. Många människor låter sina åsikter och värderingar tydligt avspeglas i sin aktivitet på Facebook och andra sociala nätverk. Det handlar inte bara om vad de skriver i sina statusuppdateringar, utan även vilka grupper de är med i, vad de ”gillar”, vilka vänner de har och vilka länkar de klickar på.

Via Google. Internetgiganten Google har över tid stora möjligheter att sammanställa en detaljerad profil över de användare som har flera av företagets tjänster och dessutom håller sig inloggade hos Google. Sökningar, surfande, mejlande till/från Gmail (både innehåll och mottagare/avsändare) och

användning av Facebook-konkurrenten Google+ hör till de aktiviteter som kan ligga till grund för sådan profilering, som sannolikt ger information om åsikter och värderingar. Ju fler av Googles tjänster en person använder desto större blir företagets profileringsmöjligheter.

Kontokortsnummer

I USA har det visat sig att kortnummer och annan information på kreditkort i vissa fall kan stjälas trådlöst med hjälp av en mobiltelefon. Det gäller kort som har beröringsfri kommunikation. Medieföretaget CBC News bevisade våren 2013 att en sådan informationsstöld är möjlig, för den som kommer nära offret, genom att använda en mobiltelefon med NFC (Near Field Communiation) och en kostnadsfri app. Stölden tog ungefär en sekund att genomföra.[26] Kortnummer kan naturligtvis även stjälas på mera traditionella vis, exempelvis via bedrägliga webbplatser och nätfiske.

Hälsa och sjukdomar

Information om hälsa och sjukdomar är oftast av känslig karaktär. Sådan information finns eller kan finnas tillgänglig på ett antal ställen. Här följer exempel på var och hur informationen skulle kunna komma ut (utöver de generella källorna).

Patientjournaler. Sjukvårdens journaler är numera digitala, och tyvärr lämnar säkerhetstänkande och integritetsskydd en hel del i övrigt att önska. ”Allt fler polisanmäls för dataintrång” skrev exempelvis tidningen Vårdfokus i april 2013,

och syftar då på vårdpersonals obehöriga läsande av patientjournaler.[27]

Surfande. Via människors surfande finns ofta möjligheter att dra slutsatser om deras hälsa och sjukdomar, eller åtminstone göra intelligenta antaganden om detta. Se ”Besökta sajter” ovan.

Sociala medier. Många människor skriver självmant om sina sjukdomar och hälsoproblem på Facebook och andra sociala medier. Medlemskap i Facebook-grupper om vissa hälsotillstånd kan också vara avslöjande, liksom ”gillande” av hälso- eller sjukdomsrelaterade företeelser. Den helhetsbild detta ger kan göra det sannolikt att en viss person har ett visst hälsotillstånd.

Trafikdata. Att exempelvis ringa eller skicka e-post till en psykoterapeut eller hjärtklinik resulterar i elektroniska fotspår som kan ligga till grund för antagandet att personen ifråga har vissa typer av hälsoproblem. I en undersökning som gjordes i Tyskland 2008 säger 52 procent av de intervjuade att de med anledning av trafikdatalagringen hos tele/internetföretag förmodligen inte skulle använda telekommunikation för kontakter med drogavvänjningsrådgivare, psykoterapeuter, relationsrådgivare och liknande.[28]

Google. Ett företag som Google har som nämnts stora möjligheter att sammanställa en profil över de användare som har flera av företagets tjänster och dessutom håller sig inloggade hos Google. I denna kan sannolikt hälsoinformation ingå.

Lyssna och titta in i bostaden

Dator. Med hjälp av ett spionprogram kan den inbyggda mikrofon och kamera (webcam) som många datorer har användas av en obehörig för att lyssna och titta in i rummet där datorn står. Det gäller så länge den är på och har internetuppkoppling. I maj 2013 åtalades en finländsk man för att ha fotograferat unga kvinnor med den inbyggda webbkameran i deras datorer, efter att ha installerat spionprogramvaror, så kallade Remote Administration Tools, på deras datorer.[29] Tidningen Hufvudstadsbladet skriver: " 'Ratting' har blivit männens och pojkarnas nya olagliga hobby på nätet. De tittar på unga kvinnor genom deras webbkameror, samlar in lättklädda bilder och spelar dem spratt."

Mobil. En mobiltelefon som försetts med en spionprogramvara kan som nämnts användas av en obehörig för att avlyssna inte bara telefonsamtal utan även rummet där telefonen befinner sig.

Teveapparat. Samsungs säljer en serie teveapparater vid namn 'Smart Hub' som har inbyggd kamera och mikrofon. År 2012 hittades en svaghet som gjorde det möjligt för hackare att aktivera dessa och därmed lyssna/titta in i rummet.[30] Ett antal företag har eller planerar teveapparater och digitalboxar med inbyggd kamera, bland annat Intel.[31] De amerikanska kabelteveföretagen Verizon och Comcast har patentsökt varsin teknologi som bygger på att människor observeras framför teven med hjälp av en digitalbox innehållande kamera, mikrofon och sensorer.[32]

Dataspel. Microsofts nya (2013) spelkonsol Xbox One har mikrofon, mörkerseende kamera och internetuppkoppling. Rent tekniskt är det därmed möjligt för Microsoft att titta och lyssna in i de bostäder där apparaten står – även när den inte används (förutsatt att sladdarna inte dras ut).[33] Och kan Microsoft titta så kan förmodligen NSA...

Biltjänst. Vissa bilar har en digital tjänst med internetuppkoppling, navigering och möjlighet att få hjälp från en central. Volvo On Call är ett sådant system. I USA har polisen vid minst ett tillfälle förmått företaget bakom den typen av biltjänst att aktivera bilens inbyggda mikrofon så att de resande kunde avlyssnas. Det skedde på distans, utan ingrepp i bilen.[34]

Elförbrukning. Genom att kontinuerligt registrera elförbrukningen hos ett hushåll går det att notera vilka elektriska apparater som används, eftersom varje apparat har sitt unika elektriska ”fingeravtryck”. Tekniken kallas Residential Power Line Surveillance.[35]

Andra digitala apparater. Explosionen av antalet digitala apparater i bostäder ger stora tekniska möjligheter att övervaka vad människor gör hemma, något som bland annat har uppmärksammats som en stor möjlighet av den amerikanska underrättelsetjänsten CIA.[36]

Utskrifter och fotokopior

Man skulle kunna tro att utskrifter från skrivare och kopior gjorda i kopieringsmaskiner är anonyma, men så är ofta inte fallet. Ett antal skrivarmodeller och kopiatorer är försedda

med en halvhemlig teknologi som förser varje utskrift/kopia med en kod, osynlig för blotta ögat, som innehåller information om bland annat apparatens serienummer och datum/klockslag för utskriften.[37] Detta möjliggör i en del fall spårning av ett papper till en viss människa, eller åtminstone till ett hushåll eller en arbetsplats.

Några specialfall

På grund av sin speciella karaktär av att vara mer eller mindre allomfattande har jag brutit ut några övervakningsinstanser och informationskällor ur ovanstående genomgång. Dessa skulle annars återkomma under samtliga ovan förekommande rubriker.

FRA. Försvarets Radioanstalt har teknisk möjlighet att i detalj gå igenom all data- och telefontrafik som passerar landets gränser. Detta ger, rent principiellt, möjlighet att ta del av många av människors innersta hemligheter (särskilt i kombination med programvaror för exempelvis mönsterigenkänning). Myndighetens digitala övervakning är omgärdad av ett detaljerat regelverk med många restriktioner. FRA har exempelvis inte tillåtelse att använda sig av information som uppstår i Sverige, skickas utomlands för bearbetning (exempelvis hos en utländsk internetbaserad tjänst) och sedan skickas tillbaka till Sverige. Den positivt sinnade utgår ifrån att FRA följer regelverket, men det saknas inte indikationer på motsatsen.[38]

NSA. Den amerikanska myndigheten för global avlyssning, National Security Agency, svävar som en osynlig ande över

allt som har med digital integritet att göra. De har som bekant mycket stora möjligheter att avlyssna och övervaka digital kommunikation, internettjänster, databaser med mera, och de har knäckt (eller skaffat sig bakdörrar till) viktiga krypteringprodukter och krypteringsprotokoll.

Allt detta underlättas av det faktum att de flesta programvaror och IT-tjänster som används – över hela världen – är av amerikanskt ursprung. Bland annat underlättas skapandet av bakdörrar (hemliga ingångar). Begreppet bakdörrar används oftast i samband med programvaror, men även hårdvara kan ha bakdörrar. Därför är det av betydelse att också en hel del hårdvara (som routrar, mobiltelefoner och datorer) är av amerikanskt ursprung. På de amerikanska myndigheter som hanterar hemlig information får inte datorer av det kinesiska märket Lenovo användas, eftersom de anses kunna ha bakdörrar inbyggda i själva hårdvaran.[39] Den misstänksamme kan tolka detta som en varning om att amerikanerna kanske själva bygger in bakdörrar i sin egen hårdvara.

Kasserade apparater. Många människor kasserar datorer, mobiltelefoner och andra digitala apparater utan att genomföra en ordentlig datarensning. Det räcker inte med att radera materialet på vanligt sätt, en särskilt raderingsprogramvara måste användas. En dator eller mobiltelefon som har använts under en tid är en veritabel guldgruva för en nyfiken obehörig om den inte rensats på ett adekvat sätt.[40] Observera att även skrivare/kopiatorer av mera avancerad modell ofta innehåller en hårddisk som kan ha kvar utskrivet/kopierat material.

Om appar. Appar är en stor riskfaktor när det gäller datasäkerhet på mobiltelefoner. Appar kan innehålla virus, spion-

program och andra slags ”elak kod”. Det är vanligt att appar överför data från mobilen till den som ligger bakom appen. I december 2010 gjorde den amerikanska tidningen Wall Street Journal en undersökning av 101 appar för att se vilka som överförde information från telefonen till annonsörer. Det visade sig att 56 av apparna överförde mobilens unika ID-nummer, 47 överförde telefonens geografiska position och 5 överförde användarens ålder, kön och andra personliga data (som telefonnummer och kontaktlista).[41]

Återidentifiering och mönsterigenkänning

Många gånger avfärdas integritetsanhängares oro inför insamling av detaljerade personliga data med att de anonymiseras innan de lagras. De tillhörande identiteterna tas alltså bort. Detta skydd av den personliga integriteten är dock inte alltid så starkt, eftersom det ibland är möjligt att återidentifiera personerna bakom informationen.

Exempelvis säger Peter Eckersley, som är doktor i datalogi och verksam vid den amerikanska medborgarrättsorganisationen Electronic Frontier Foundation, att det räcker med kännedom om en människas kön, postnummer och födelsedag (årtal krävs inte) för att unikt kunna identifiera honom eller henne. Generellt är det så att när flera urvalskriterier kombineras blir det ofta bara en enda person kvar i den grupp som uppfyller alla krav.

Ett exempel: Om en person skulle skaffa en ny och anonym mobiltelefon, tillsammans med ett nytt och anonymt SIM-kort, och sedan fortsätter att ringa och skicka sms som vanligt så är det tekniskt möjligt för teleoperatören att identifiera personen via kontaktmönstret. Samkörning med tidigare lagrad

information om identifierade kunders kontaktmönster visar då att det bara finns en enda person för vilket kontaktmönstret överensstämmer. Förfarandet kallas mönsterigenkänning.

Man behöver inte ens ringa. Forskare vid Massachusetts Institute of Technology har kommit fram till att människors förflyttningar, så som de kan mätas via deras mobiltelefoner, är så unika att det räcker med fyra mätningar (bestående av tid och plats) för att identifiera en viss människa.[42]

Vid avslöjandet av den av säkerhetsskäl mycket känsliga kärleksförbindelsen mellan den dåvarande amerikanske CIA-chefen och fyrstjärnige generalen David Petraeus och författaren Paula Broadwell lyckades FBI knyta komprometterande e-postmeddelanden till Broadwell trots att hon vidtagit långtgående försiktighetsåtgärder för att anonymisera sig. Hon använde ett anonymt Gmail- konto, och hon loggade aldrig in på det från sin bostad eller arbetsplats, utan bara när hon var anonymt uppkopplad via ett trådlöst nätverk på något av de hotell hon bodde på. Via Gmail hade FBI tillgång till de IP-nummer som använts för att komma åt kontot. Dessa gick till ett antal hotell, dock helt utan personlig information. Men FBI samkörde de aktuella hotellens gästlistor för de dagar då inloggning på Gmail hade gjorts, och det var bara ett namn som hela tiden återkom: Paula Broadwell.[43]

4. Betydelsen av NSA:s spionage

Under 2013 har världen skakats av en serie avslöjanden om hur långtgående den amerikanska övervakningen och avlyssningen är. Det handlar om USA:s myndighet för global avlyssning, National Security Agency (NSA), som genom visselblåsaren Edward Snowdens förtjänst har avslöjats som en global bläckfisk vars öron- och ögonförsedda tentakler tränger in i de flesta av IT- samhällets skrymslen och vrår.

Många kanske tänker att NSA utgör ett hot för terrorister och grov organiserad brottslighet – och det är bra – men att ”vanliga” människor knappast berörs. Det är emellertid fel, av flera skäl.

För det första kan man konstatera att det amerikanska spionaget riktar sig mot en mycket bredare målgrupp än terrorister och maffiagrupper. Politiker och politiska institutioner i många länder står säkerligen under amerikansk övervakning, liksom företag som är eller kan bli intressanta i ett större sammanhang (genom att vara stora på marknaden eller genom att ha någon särskild tillgång, såsom spetsteknologi).

För den som tänker med ett par stegs framförhållning är det uppenbart att detta stärker USA och amerikanska intressen, och att det oftast sker på bekostnad av andra länder och deras intressen. Om USA exempelvis kan nå bättre resultat

i en politisk förhandling med andra länder på grund av sitt spionage så blir ju avtalet sämre för de andra länderna, vilket i förlängningen drabbar deras medborgare.

Om NSA gör dataintrång hos icke-amerikanska företag som är med och bjuder i stora internationella upphandlingar och sedan delar med sig av de inhämtade affärshemligheterna till de amerikanska företag som kämpar i samma upphandling så ökar naturligtvis sannolikheten för att något av de amerikanska företagen tar hem ordern. Och då drabbas de avlyssnade företagen av ett ekonomiskt bakslag, som i förlängningen fortplantar sig i de aktuella länderna. Det handlar alltså om att överföra sysselsättning och välstånd från andra länder till USA. Effekten blir densamma om NSA inhämtar information om icke-amerikanska företags eller forskningsinstitutioners spetsteknologi och lämnar över materialet till amerikanska företag.

Den som tvivlar på att NSA:s dataintrång, spionage och avlyssning riktar sig mot andra länders politiska institutioner/ledare och andra länders företag rekommenderas att läsa dokumentet ”Amerikansk avlyssning från Echelon till Prism”. Detta utgörs av två kapitel ur min bok ”Övervakad”, som utkom på Liber förlag men nu är slut på förlaget. Det fritt tillgängliga dokumentet finns på Den Nya Välfärdens webbplats under fliken ”Integritetsombudsmannen” (du kan också googla fram det).

Eftersom NSA:s verksamhet delvis handlar om överföring av välstånd berör den oss alla. Det blir inte mindre sant av att effekten inte kan mätas, vilket däremot tyvärr skapar ett pedagogiskt problem. Det är lättare att bortse från det man inte tydligt kan se och mäta.

NSA:s ohemula nyfikenhet och avsaknad av moral orsakar dock även andra typer av skador. Vad de har gjort är inget mindre än att angripa IT-samhällets själ. De har försvagat internationella standarder för kryptering, övertalat eller pressat teknikföretag att bygga in bakdörrar eller försvagningar i sina krypteringsprogram och andra produkter, försett gigantiska undervattenskablar med avlyssningsanordningar, byggt avlyssningsgränssnitt mot de digitala nätverken på många andra platser, och skaffat sig tillgång till innehåll som människor över hela världen i förtroende har lämnat över till företag som Facebook och Google.

Som ett resultat av detta har nu förtroendet för det moderna samhällets digitala infrastruktur till stor del fallit bort. Det ställer till med stora problem för företag, stater och andra. Hur ska databehandling, kommunikation och datalagring egentligen gå till när nästan varenda sladdstump kan misstänkas ha öron? När man inte ens kan lita på de stora världsledande leverantörerna av hårdvara, mjukvara och tjänster? När det verkar vara på gränsen till omöjligt att sända konfidentiell information utan risk för att den snappas upp av obehöriga?

Resultatet kan bli ökade kostnader för de enskilda företagen och organisationerna, och en bromskloss på all verksamhet som är av känslig natur. I förlängningen kan det leda till lägre tillväxt. Allt går helt enkelt trögare i en värld där man måste misstro den digitala infrastrukturen. I skrivande stund (september 2013) har vi knappt hunnit se resultaten av detta, men två exempel har nyligen visat sig.

I Frankrike har premiärministerkontoret förbjudit ministrarna att använda andra mobiltelefoner än Toerem, som tillverkas av det franska företaget Thales, när de avhandlar

konfidentiella frågor.[44] Reaktionen är naturlig, men sorglig. I förlängningen kan man ana risken för en slags avlyssningsbetingad protektionism, där små företag i många olika länder tillverkar dåliga produkter (eller dåliga tjänster) till höga priser. Alla är förlorare på den utvecklingen.

Det andra exemplet kommer från Brasilien, där president Dilma Rousseff förbereder lagstiftning om att utländska IT-företag måste förlägga sina datacentraler till Brasilien om de vill vara verksamma i landet.[45] Att på det viset försöka skydda sin information genom att hålla den inom landet är en naturlig reaktion. Tyvärr går den helt på tvärs mot IT-samhället själ. Internet och den digitala infrastrukturen blir effektiv bara när gränser fritt kan korsas och geografin helt enkelt ignoreras. Det är så IT fungerar. Länders och företags berättigade strävan efter att undgå den amerikanska bläckfisken riskerar alltså att driva fram en utveckling som flyttar oss tio eller tjugo år bakåt i tiden, och försämrar möjligheterna till tillväxt och innovation. Detta är en viktig del av den skada som NSA har förorsakat världen.

Nationalism, protektionism och en bromskloss på ekonomiska aktiviteten är alltså företeelser som vi kan komma att ha NSA att tacka för.

Men det räcker inte med detta. Ytterligare en skada som NSA förorsakat är att de aktivt har försämrat säkerheten på internet. De svagheter i krypteringsprotokoll och krypteringsprodukter och andra slags bakdörrar som NSA har drivit fram kan komma att upptäckas och utnyttjas av organiserad brottslighet, terrorister och andra ljusskygga grupper. Om så sker har vi verkligen hamnat ur askan i elden.

Det brustna förtroendet för internet och den digitala världens övriga infrastruktur kan också få andra konsekvenser

än de ovan nämnda. I många länder har man exempelvis diskuterat införandet av så kallad e-röstning (e-demokrati), alltså att rösta via internet. Är det efter NSA- skandalen verkligen möjligt att skapa det förtroende för de tekniska lösningarna som krävs för att möjliggöra detta? Vågar människor exempelvis lita på att valhemligheten är garanterad vid e- röstning?

Låt oss gå till nästa risk med NSA:s övervakning. Tänk om Edward Snowden istället för att lämna ut information om övervakningssystemen till pressen hade använt avlyssnad information om människor för att berika sig själv? Om man har tillgång till stora delar av världens e-post, surfande, sms:ande, facebook:ande och liknande har man också väldiga möjligheter att ägna sig åt exempelvis utpressning. Den information som NSA:s olika system kan ta fram skulle också kunna användas av en omoralisk person för att göra exceptionellt goda affärer på börsen (med hjälp av insiderinformation). Uppfinningar skulle kunna stjälas och kanske säljas. Listan kan nog göras lång. Via bakdörrar är det också möjligt att fjärrstyra människors datorer, vilket exempelvis skulle kunna användas för att sätta dit människor för brott de inte har begått.

Detta aktualiserar frågan hur många personer det finns som kan koppla in sig till bläckfiskens öron och ögon. Edward Snowden kunde det, trots att han hade en relativt låg position hos NSA:s underentreprenör Booz Allen Hamilton. Enligt nyhetstjänsten ZDnet finns det ungefär 1000 personer inom NSA (inklusive dess underentreprenörer) som liksom Edward Snowden har behörighet som systemadministratör. Enligt ZDnet har dock även personer som saknar denna behörighet – en större grupp – tillgång till NSA:s hemliga data.[46] Ingen siffra anges. Man kan också konstatera att det i USA

finns 1,4 miljoner människor med säkerhetsklassningen ”top secret”, vilket är den högsta klassningen och den som Edward Snowden hade.[47]

Det finns alltså väldigt många potentiella läckor, och det räcker egentligen med en enda för att orsaka stor skada för de människor vars avlyssnade data blir missbrukade. Något som ökar oron är att Edward Snowden kunde ladda ned ett så stort antal topphemliga dokument utan att systemets inbyggda varningsklockor ringde. Det tyder på en låg säkerhetsnivå – på en plats där säkerheten borde vara extremt hög.

Nästa risk är att NSA:s framspionerade information hamnar i orätta händer genom intrång utifrån; hackerattacker. Den som helt avfärdar möjligheten att en myndighet som NSA skulle kunna bli hackad rekommenderas att läsa kapitlet ”Exempel på intrång och dataläckor” längre fram i denna bok.

Det finns en diskussion om huruvida vi i världen utanför USA ska bemöta det amerikanska spionaget mot oss med tekniska eller politiska medel. Det senare har förslagits av vissa europeiska politiker, som vill träffa en överenskommelse med amerikanerna om att de ska sluta spionera på oss. Sådana tankar måste avfärdas som löjeväckande. Kanske rör det sig bara om ett spel för gallerierna, som syftar till att lugna medborgarna och få slut på debatten. Till saken hör att en del länders säkerhetstjänster har fingrarna i syltburken tillsammans med NSA, som de samarbetar med (dit hör Sverige). Dessa verkar ha en dubbel roll som både offer och partner.

Jag skulle vilja avsluta detta avsnitt med att måla upp ett riktigt skräckscenario. Det resonemanget vill jag inleda med att påminna om den legendariska FBI-chefen J. Edgar Hoover. Han var chef för den amerikanska federala polisen FBI i 48 år, från 1924 till 1972, under åtta presidenter. Varför satt han

så länge? Jo, alla var rädda för honom eftersom han satt på så mycket komprometterande information om i princip alla makthavare. Inte ens presidenter vågade utmana J. Edgar Hoover, så han blev kvar på sin post tills han avgick med döden.[48]

Tänk om denne psykopat hade levt idag och varit chef för NSA? Tanken svindlar. Han hade sannolikt kunnat skaffa sig tillgång till mycket större mängder komprometterande information än Hoover gjorde under 1900-talet. Kanske hade J. Edgar Hoover i 2000-talsversion, som chef för NSA, i det fördolda mer eller mindre kunnat styra hela USA genom hot och utpressning. Vid närmare eftertanke, skulle det verkligen krävas att han eller hon var *chef* för NSA? Och vid nästa eftertanke, är det bara USA som han eller hon skulle kunna styra?

Man kan fråga sig – har ens amerikanerna själva förstått vilket monster de har skapat?

5. Integritetshot som väntar runt hörnet

Som om inte de befintliga hoten mot den personliga integriteten skulle vara nog kan man konstatera att ett antal nya sådana kan anas runt hörnet. Bakomliggande drivkrafter är den tekniska, marknadsmässiga och politiska utvecklingen. Här följer några företeelser som jag i det sammanhanget skulle vilja fästa uppmärksamheten på.

Det kontantlösa samhället. Man har länge pratat om ”det kontantlösa samhället” som en tänkbar (fin) framtidsvision, men när det nu har börjat dyka upp kontaktlösa butiker känns scenariot inte längre så avlägset. Om och när människor inte längre kan genomföra vardagliga betalningar med den anonymitet som sedlar och mynt ger så är den personliga integriteten död. Då kan man inte ens köpa en veckotidning eller en dosa snus utan att det registreras i databaser. Våra betalningar utgör en närmast total spegelbild av våra liv.

Big data. ”Big data” är information som uppstår i riktigt stora databaser med riktigt stort underlag. Det kan röra sig om telebolags data om kundernas trafik, stora e-handelssajters data om vad kunder tittar på och vad de beställer, och biltullars information om passerande fordon. Ett paradexempel

är förstås Googles information om sökningar, ett annat är Facebook. Genom att samköra olika ”big data”-register, och/eller använda programvaror för mönsterigenkänning, kan oväntade och långtgående integritetshot uppstå. Ökad användning och tilltagande kommersialisering av ”big data” betraktas inom IT-branschen som en av de så kallade megatrenderna. Försäkringsbolag, banker, kreditbedömare, skattemyndigheter och försäkringskassan hör till dem som skulle ha mycket att vinna på användning av personuppgifter sprungna ur ”big data”.

Smarta kameror. Dagens övervakningskameror, som i de flesta fall är ”dumma”, är enligt mitt förmenande aningen övervärderade som integritetshot. Situationen förändras dock radikalt när kamerorna blir ”smarta” och kopplas till databaser, en utveckling som redan kommit en bra bit på väg. I Sverige har vi redan på vissa håll (bland annat i biltullarna) automatisk inläsning av bilars nummerplåtar, vilket gör att människors förflyttningar automatiskt, i masskala, hamnar i databaser. Vid horisonten kan man ana ett tänkbart samhälle där kameror med automatisk ansiktsigenkänning på motsvarande sätt lagrar information i databaser om var människor befinner sig.

Övervakade bilar. Risken är överhängande att våra resor med bil kommer att vara övervakade och registrerade i framtid som inte ligger så långt bort. De ovan nämnda smarta kamerorna är inte det enda hotet. Ett minst lika stort hot är GPS-baserad vägskatt, försäkring och fartövervakning – att både plats och fart kontinuerligt samlas in med GPS-hjälp och via mobiltelefonnäten sänds över till myndigheter och

andra aktörer. Ytterligare ett stort hot är de kommersiella digitala tjänster som inom kort kommer att vara en integrerad och självklar del i nya bilar. Många av dem kommer att innehålla geografisk positionering, vilket tillsammans med bilens möjlighet att sända data via mobiltelefonnätet skapar ett stort integritetshot.

Radioetiketter. Så kallade radioetiketter (RFID) börjar få stort genomslag i samhället. Sådana finns, eller kommer snart att finnas, på exempelvis kollektivtrafikkort, kreditkort, diverse inpasseringskort och biblioteksböcker. Tester görs med RFID i kläder.[49] Det ”farliga” med dessa kretsar är att de är trådlösa (viket förstås också är hela vitsen med dem). Som nämnts har larmrapporter kommit om att bedragare i situationer där trängsel råder kan läsa av nummer och andra data på människors kontokort genom att ha en apparat med en liten antenn under jackan.[50] Vad händer om snokar på motsvarande sätt kan läsa av vilka böcker personen intill på bussen har i sin väska? Eller om butiker sätter upp antenner vid ingången som läser av kundernas RFID- försedda föremål? En grupp IBM-anställda har sökt patent på en teknologi för att göra det.[51]

Uppkopplade apparater. Marknadsekonomi och framväxten av allt fler internetuppkopplade apparater är en fatal kombination för den personliga integriteten. Företagens väldiga (och fullt berättigade) strävan efter ökad lönsamhet, vilket vanligtvis sker via ökad försäljning, skapar oerhörda incitament för att samla in detaljer om konsumenter. Det är ju lättare att sälja om man vet vad kunden är intresserad av. När insamling och lagring av nya slags elektroniska fotspår blir möjlig genom att vi använder fler och nya slags apparater

som är internetuppkopplade kan frestelsen för företagen bli övermäktig. Vad kan det vara för apparater? Tänk badrumsvågen, bilen, kameran, mikrovågsugnen, tvättmaskinen, värmepumpen, teveapparaten...

Kroppsmätning. En företeelse i tillväxt är kroppsmätning, vilket utgör en del i det som på engelska kallas ”quantified self” (egenmätning). Det handlar om att sensorer mäter exempelvis hjärtrytm och blodets syresättning, lagrar informationen för framtiden och i många fall erbjuder möjligheten att dela den i sociala nätverk. Sömnmätning går till på ungefär samma sätt – djupet i sömnen mäts minut för minut, ofta kombinerat med snarkningsdetektor och gå-på-toaletten-registrering. Tala om intim information! Tänk om försäkringsbolag eller arbetsgivare får tillgång till sådana kroppsdata? I USA förekommer det redan att anställda uppmuntras att ladda upp data från sin egenmätning till arbetsgivarens databas.[52]

Livsloggning. En annan framväxande företeelse som är besläktad med kroppsmätning är livsloggning; att ständigt bära en kamera som automatiskt tar ett par bilder i minuten och lagrar dem komplett med geografisk position. En av många intressanta frågor är hur rättsväsendet påverkas om livsloggning blir vanligt. Tänk om det kommer att anses suspekt att stänga av livsloggningen (”du måste ju ha något att dölja”)? Det svenska företaget Memoto håller på att utveckla en livsloggningskamera med tillhörande lagringstjänst. Alla bilder, komplett med geografisk position, ska lagras på Memotos servrar.[53] Kommer NSA att ha fingrarna i den syltburken?

Google Glass. Här passar det att som ett exempel nämna Google Glass, ett slags glasögon utan glas som projicerar information på ögat. Produkten testas nu och ska släppas under 2014. Med kamera, mikrofon, internetuppkoppling och så kallad augmented reality ger Google Glass väldiga möjligheter, inte bara att nästan omärkligt fotografera och filma människor. Skulle man lägga till automatisk ansiktsigenkänning vore integritetsmardrömmen total. Kanske kommer man på sikt att kunna få namn och inkomstuppgift om främlingar man träffar på krogen, hängande som små skyltar över deras ansikten, diskret projicerat av glasögonen mot ögat?

Europeisk brottsbekämpning. I ett nytt betänkande, ”Europarådets konvention om IT-relaterad brottslighet”, kommer Europarådet med ett mycket integritetsfarligt förslag. Tanken är att systemoperatörer, alltså personal i datacentraler, skall kunna tvingas att lämna ut information ur systemen till polisen – i hemlighet, utan rätt att avslöja detta för sina arbetsgivare.[54] Hemliga och munkavleförsedda polisspioner alltså. Detta är bara ett exempel på integritets- eller frihetshotande förslag från de olika europeiska institutionerna. Tidigare har vi bland annat begåvats med det starkt integritetskränkande Datalagringsdirektivet. Fler, och värre, förslag kan förväntas.

Nya terrorattentat. Ett nytt terrorattentat av en magnitud lika stor som eller större än 11 september-attackerna skulle kunna skapa en politisk situation där övervakningsåtgärder av drakonisk karaktär införs; övervakningsåtgärder som idag vore otänkbara. Och då lever vi ändå idag med en övervakning som i sin tur hade varit otänkbar före 11 september-attentaten...

Automated law enforcement. Ett bra begrepp på svenska saknas, men det engelska ”automated law enforcement” innebär en automatisering av polisens arbete: Att programvaror hela tiden går igenom alla människors elektroniska fotspår på ständig jakt efter brott och regelöverträdelser. I vissa utländska poliskretsar framställs detta som framtidens melodi. Ett exempel: Den som passerar biltullarna samma tid varje morgon och kväll trots att vederbörande är sjukskriven kan misstänkas för fusk.

NSA. Kommentarer överflödiga. Se för övrigt separat kapitel om NSA.

6. Varför dog integritetsfrågan i svensk debatt?

Integritetsfrågan i svensk politik dog efter FRA-debatten. Varför, kan man fråga sig? Den digitala revolutionen rullar ju vidare, loggfilerna bara ökar i antal och det politiska intresset för att använda dem i övervakningssyfte tilltar. Digitala fotspår uppstår på allt fler områden, samtidigt som de blir allt djupare och intimare till sin karaktär. Den matematiska nörden skulle kalla det en kvadratisk tillväxt för Storebror.

Ändå är frågan död, åtminstone på den stora nationella scenen. Ingen politiker tar längre upp saken, än mindre något politiskt parti (förutom Piratpartiet), och inga organiserade protester eller demonstrationer förekommer. Vad kan det bero på?

För det första måste man konstatera att integritetsfrågan inte bara *dog* efter FRA-debatten, den *föddes* också med FRA-debatten. Åtminstone i de breda kretsarna. Före FRA-debatten var det få som tänkte på Storebror, så vi har ingen tradition av integritetsdebatt att falla tillbaka på. Om man inte går riktigt långt tillbaka i tiden, förstås.

De som varit med ett tag minns de stora protesterna på 1980-talet när svenska myndigheter skulle genomföra en så kallad folkräkning. Debattens vågor gick höga, och många bojkottade folkräkningen. Den ansågs vara djupt integritets-

kränkande. Men de data som då samlades in utgör ett spott i Ålands hav jämfört med de digitala data som idag samlas in om oss av myndigheter och företag.

Här följer några tänkbara förklaringar till det bristande intresset för de tilltagande hoten mot den personliga integriteten.

Tillvänjning. Utvecklingen har gått successivt, och vi fungerar kanske som grodan i det kinesiska talesättet: Om en groda slängs i varmt vatten hoppar den ur, men slängs den i kallt vatten som sedan värms upp blir den allt slöare tills den slutligen blir kokt.

Bekvämlighet. Det är bekvämt och spar tid att strunta i sin integritet. All form av anonymisering, även enkel sådan, är omständlig. Att radera cookies, logga ut från olika tjänster mellan användningstillfällena, kryptera information och vidta andra skyddsåtgärder tar tid. Vidare är det bekvämt att webbplatser känner igen mig sedan förra besöket och snabbt visar information som är relevant för just mig. Det är tryggt att registrera kollektivtrafikkortet med namn och personnummer (och därmed göra mig geografiskt spårbar) eftersom jag då får ett nytt om jag tappar kortet. Och så vidare...

Snålhet. Om man får någon procents rabatt på sina inköp vill man förstås gärna dela med sig av inköpsvanorna, in i minsta detalj, till Den Stora Detaljistkedjan. Eller hur? För integritet får väl inte kosta pengar? Ursäkta raljerandet, men snålhet är en av integritetens stora fiender. Här passar det bra att nämna det kloka talesättet: ”Om något är gratis på nätet är det du som är produkten”. Det är mitt i prick. Lite hårdraget kan

man säga att vi människor får den personliga integritet vi är beredda att betala för.

Delande. Sociala nätverk som Facebook erbjuder användarna stora fördelar, och lockar därmed människor att strunta i hotet mot integriteten. Detta skapar i sin tur en tillvänjning.

Generationsväxling. Själv tillhör jag de digitala immigranterna, människor som inte är födda i IT-samhället. Våra referensramar utgörs av en värld där man exempelvis kunde gå in i en telefonhytt var som helst och ringa ett samtal under 100 procents anonymitet. Verkligen hundra procents anonymitet, något som är mycket svårt att uppnå idag. En allt större del av befolkningen är emellertid digitala infödingar – de är uppväxta i internetsamhället där allt loggas. Och den hemska sanningen (?) kanske är: They don't care. Tecknen är många på att unga människor ofta tar mycket lätt på integritetsproblemet – om de över huvud taget ser det som ett problem.

Det händer inte mig. De flesta är nog medvetna om att man kan råka illa ut med anledning av sina elektroniska fotspår, men de flesta undrar: Varför skulle det hända just mig? De flesta av oss känner ingen som blivit allvarligt drabbad, eller över huvud taget drabbad, på integritetsområdet. Då är det väl ingen stor grej?

Staten är snäll. Vi svenskar har av tradition ett väldigt stort förtroende för staten. Skillnaden är stor gentemot människor som har bott i länder som har, eller har haft, krig eller diktatur. Varningen att dagens IT-samhälle hade varit rena paradiset för Stasi eller Gestapo, och att vi inte vet hur snäll

den svenska staten är imorgon, bemöts ofta med ett skratt och en anklagelse om att vara ”foliehatt”.

Uppgivenhet. Ibland tror jag att ren uppgivenhet är en väsentlig del i förklaringen till det bristande intresset för personlig integritet. Det är ändå kört, resonerar många. Man kan konstatera att det resonemanget är självförverkligande.

Rädsla for terrorism. Människor är rädda för terrordåd, och den rädslan har underblåsts av politiska och polisiära krafter som redan före de spektakulära terrordåden 2001 ville införa ökad övervakning, inskränka medborgerliga rättigheter och över huvud taget låta staten breda ut sig på medborgarnas bekostnad. Delvis är rädslan rentav skapad av våra politiska ledare. Observera att jag inte förnekar existensen av hotet från terrorismen, men jag tror att risken överdrivs, att värdet i digital massövervakning som skyddsmedel övervärderas och att regeringar har utnyttjat situationen. Psykologer har länge vetat att människor har en tendens att överskatta spektakulära men osannolika risker medan de underskattar vardagliga risker som är betydligt mera sannolika.

Om svenska politiker

Hösten 2013 fick vi en del av förklaringen till svenska politikers bristande intresse för integritetsfrågan, när den grävande journalisten Duncan Campbell[55] avslöjade att Sverige är NSA:s viktigaste samarbetspartner i Europa efter Storbritannien. Ett ännu viktigare skäl till att de politiska partierna i Sverige inte driver integritetsfrågan är dock sannolikt att de inte känner något tryck underifrån. De tror inte att ett reellt

engagemang i integritetsfrågan skulle hjälpa dem att vinna nästa val. Och det är nog, tyvärr, en korrekt bedömning.

7. Exempel på intrång och dataläckor

Aningen förenklat kan man säga: Alla databaser läcker. Kanske har du som läser detta känslig information i en databas som blivit hackad – de flesta intrång kommer aldrig till allmänhetens kännedom.

Det finns tre huvudsätt på vilka informationen kan få spridning till obehöriga: Genom intrång utifrån (hackning), genom personalens åtgärder (avsiktliga eller oavsiktliga) och genom tekniska fel (buggar). Ett antal exempel ur de tre kategorierna listas nedan. Observera att det bara rör sig om ett axplock. Medborgarrättsorganisationen Privacy Rights har lagt ut en sökbar databas över stora dataläckor som kommit ut i offentligheten.[56]

A. Angrepp utifrån

Obehöriga personer, ofta kallade hackare, kan lyckas ta sig in i databaserna utifrån. Detta sker hela tiden. Stora företag tystar ofta ned dataintrång (liksom andra dataläckor) av rädsla för att tappa image.[57] På senare tid har hackare i ökande utsträckning börjat genomföra dataintrång i ekonomiskt syfte, istället för att bara visa sig på styva linan. ”Mer än någonsin tidigare är databrottslingarna i dag ute efter dig personligen” skriver

exempelvis Svenska Dagbladet (16/4 2013) i en artikel med rubriken ”Kartlägger allt du gör på nätet”.

En undersökning som presenterades sommaren 2013 visar att svenska myndigheter har dålig IT- säkerhet. Dels är skyddet mot attacker utifrån dåligt, dels finns ett stort problem i att personalen inte följer säkerhetspolicyn.[58]

Nedan följer ett antal exempel på hackerintrång:

Svenskt jättehack. Sommaren 2013 dömdes Gottfrid Svartholm Warg till fängelse för två dataintrång. I det ena intrånget skaffade han sig via IT-företaget Logica (numera CGI) tillgång till Skatteverkets SPAR-register (ett register över hela den svenska befolkningen) och Kronofogdens register. Han skaffade sig också tillgång till information om människor med skyddade personuppgifter, liksom känslig information om 20.000 poliser och en del annat. Det andra intrånget gjordes hos Nordea, och syftade till att överföra pengar från andra människors bankkonton. Gottfrid Svartholm Warg har överklagat domen.[59] Han misstänks också av den danska polisen för att via IT- driftsföretaget CSC ha tagit sig in i databaser tillhöriga flera danska myndigheter. Exempelvis ska han ha kommit över ett register över människor som är efterlysta genom EU:s gränssamarbete Schengen.[60] Gottfrid Svartholm Warg säger sig vara oskyldig till alla intrång – han hävdar att dessa visserligen skett från hans dator men att datorn blivit kapad av någon annan som fjärrstyrt den.

Tysk teleoperatör hackad. I september 2013 stals personuppgifter för mer än 2 miljoner kunder till den tyska teleoperatören Vodafone Germany. Det rör sig om namn, adresser, bankkontonummer och födelsedatum. Vodafone varnar nu

sina kunder för att den stulna informationen kan användas för nätfiske.[61]

Twitter hackat. Twitter drabbades 2013 av ett intrång varvid angriparna kan ha kommit över 250.000 personers användaruppgifter.[62]

Jättehack mot Apple. En grupp hackare verkar år 2012 ha kommit åt data om 12 miljoner Apple-användare genom att ta sig in i FBI:s datorer. Apple kommenterar inte uppgifterna och FBI dementerar att deras datorer skulle ha utsatts för ett intrång, men flera experter på cyberbrott bekräftar uppgifterna.[63]

Jättehack mot Sony. Det japanska företaget Sony drabbades 2011 av ett stort dataintrång där 100 miljoner användare av spelkonsolen Playstation fick sina konton hackade. Dessutom stals 12.700 kredit- och kontokortsnummer.[64]

Spionprogramvara på bibliotek. En okänd person installerade under 2011 en spionprogramvara, en så kallad keylogger, på flera datorer på biblioteket i Sunne. Därmed kunde den obehöriga exempelvis komma åt alla inloggningsuppgifter som användare matade in.[65]

Hundratusentals patientuppgifter hackade. Det avslöjades 2012 att hackernätverket Anonymous genomfört ett intrång hos Västra Götalandsregionen och kan ha kommit åt hundratusentals patientuppgifter. Det handlar om sekretessbelagd information från tidigt 1990-tal och fram till 2009.[66]

Jobbsökarsajt hackad. Den svenska jobbsökarsajten Monster har drabbats av två stora dataintrång. År 2007 stals uppgifter om 1,3 miljoner jobbsökande som lagt in sin CV i databasen. År 2009 skedde ett nytt intrång.[67]

Kortföretag hackat. Det amerikanska kortföretaget Citi Credit Card, tillhörigt Citigroup, drabbades 2011 av ett dataintrång där obehöriga kom över namn, kontonummer och kontaktinformation om 360.000 kunder.[68]

100 miljoner kortnummer hackade. En attack mot finansföretaget American Heartland Payment åren 2005-2007 exponerade 170 miljoner kreditkortsnummer för obehöriga. Det är ett av världshistoriens värsta dataintrång.[69]

Pojke hackade Pentagon. En brittisk 16-åring lyckades 1995 hacka sig in hos Pentagon, närmare bestämt ”United States defence and missile systems”. Han fick bland annat tillgång till forskning om ballistiska vapen, flygplanskonstruktion, lönelistor, data om anställda samt e-post, och han raderade filer om stridsledning och artificiell intelligens. Amerikanerna trodde först att angreppet gjorts av främmande makt, och sa att den aktuella ”spionen” hade ”orsakat mer skada än KGB”. Hackaren beskrevs som ”det främsta hotet mot USA:s säkerhet”.[70]

Pojke hackade NASA och Pentagon. En 15-årig pojke hackade sig 1999 in i datorerna hos den amerikanska rymdflygstyrelsen NASA, vilket orsakade 21 dagars stillestånd för datorer som stödde den internationella rymdstationen. Bland annat laddade han ned den programvara som reglerar temperatur

och luftfuktighet i rymdstationen. Pojken tog sig också in i ett vapensystem hos Pentagon.[71]

UFO-entusiast hackade NASA och Pentagon. En arbetslös autistisk 42-åring som sökte bevis för existensen av så kallade UFO:n (flygande tefat) hackade sig 2001-2002 in i datorer hos Pentagon och NASA. Intrånget, som pågick under 13 månader, har kallats ”det största militära dataintrånget någonsin” [72].

B. Läckor orsakade av personalen

Den personal som är satt att sköta en databas kan vara korrupt, nyfiken eller slarvig med säkerhetsrutinerna. Anställda kan frestas att använda känslig information för egna syften, eller sälja den. Ibland är det istället misstag från personalens sida som ligger bakom läckorna. Det förekommer också att företagsledningen missbrukar databaser. Här följer ett antal exempel på läckor orsakade av personal eller företagsledning.

Soldat bakom historiens största dataläcka. Den amerikanska soldaten Bradley Manning (numera Chelsea Manning) lämnade år 2010 över flera hundra tusen hemliga militära och diplomatiska dokument till Wikileaks. Det har kallats historiens största läcka av information till allmänheten. Det faktum att Manning trots sin låga militära rang hade tillgång till sådana enorma mängder topphemligt material, liksom att det var tekniskt möjligt för honom att helt enkelt kopiera över dem till sin kameras minneskort och gå hem med detta, visar hur låg säkerhetsnivån var.

Jätteläcka drabbade NSA. Underrättelseanalytikern Edward Snowden lämnade sommaren 2013 över ett mycket stort antal topphemliga NSA-dokument till bland annat den brittiska tidningen Guardian.

Teleoperatör missbrukade egna loggfiler. När styrelsen för den stora tyska teleoperatören Deutsche Telekom, Tysklands motsvarighet till Telia, trodde att en styrelseledamot läckte affärsinformation till pressen tog de till extraordinära åtgärder. För att få reda på vem det var analyserades loggfiler för styrelseledamöter och kända journalister, för att ta reda på vilka nummer de ringt och vilka de blivit uppringda av. Styrelsen använde också Deutsche Telekoms lagrade data om mobiltelefoners geografiska position för att försöka avslöja eventuella möten mellan styrelseledamöter och journalister.[73]

Kvinnojourens dator glömdes i butik. Sommaren 2013 glömde verksamhetschefen vid en kvinnojour i Skåne en bärbar dator med sekretessbelagd information i en butik. När det upptäcktes var datorn borta. Den spärr som finns på datorn kan kringgås med viss datakunskap, skriver tidningen Metro.[74]

Missbruk på Försäkringskassan. Fyra anställda på Försäkringskassan prickades 2013 för dataintrång i interna register. De gjorde sammanlagt 57 sökningar i ärenden de inte hade behörighet för.[75]

Socionom missbrukade register. En socionom vid stadsdelsförvaltningen i Malmö har 2013 polisanmälts misstänkt för att vid ett 20-tal tillfällen under ett års tid ha gått in i register

och tagit del av information som inte hade med hennes tjänsteutövning att göra. Kvinnan har avskedats.[76]

Polis missbrukade register. En polis i Bohuslän dömdes 2013 för att vid tre tillfällen ha använt olika polisregister för att söka information om en kollega och dennes familj.[77]

Läkare polisanmäld för dataintrång. En läkare i Värmland polisanmäldes under 2013 för att vid minst 30 tillfällen ha gjort sig skyldig till dataintrång i vårdens system.[78]

Vårdchef polisanmäld för dataintrång. En chef vid en av landstingets vårdinrättningar i Linköping polisanmäldes 2013 för dataintrång.[79]

Läkare dömd för dataintrång. En läkare i Kronobergs län dömdes 2012 till böter för att vid minst 21 tillfällen ha tagit del av en patients journal trots att de inte hade någon vårdrelation.[80]

Läkare åtalas för dataintrång. En läkare vid Akademiska Sjukhuset i Uppsala åtalades 2012 för att ha sökt information i patientjournaler i syfte att smutskasta en patient.[81]

Läkare snokade i rivalens gynjournal. En överläkare som låg i skilsmässa dömdes 2012 för dataintrång efter att ha gått in i den gynekologiska journalen för hennes exmans nya kvinna.[82]

Läkare försökte kartlägga invandrarkvinnors sexliv? En läkare dömdes 2013 för att ha gjort 177 olagliga sökningar i unga invandrarkvinnors journaler på kvinnokliniken. Han miss-

tänks för att på föräldrars uppdrag ha försökt kartlägga deras döttrars sexualliv.[83]

Äldreomsorgen i Laholm. En anställd vid äldreomsorgen i Laholms kommun anklagades 2013 för att olovligen ha gått in i äldreomsorgens datasystem. Åklagaren ska inleda en förundersökning.[84]

Sökmotor läckte sökningar. År 2006 råkade det amerikanska internetföretaget America Online (AOL) ut för en spektakulär dataläcka. Det var personalen som av misstag la ut ett register med 20 miljoner sökmotorsökningar på internet. Filen togs bort snabbt men var då redan kopierad och spridd över nätet. Läckan innehöll information om söktermer och vilka kundnummer på AOL som gjort respektive sökning. Det tog inte lång tid för tidningen New York Times att i reportagesyfte ta redan på namnet bakom ett av kundnumren.[85]

Teleoperatör bestulen på datorer. Det irländska telekomföretaget Eircom blev 2012 bestulet på tre bärbara datorer, varav två stals från kontoret och en från en anställds bostad. Därmed fick obehöriga tillgång till finansiell information om 6.845 kunder och 686 anställda.[86]

Personuppgifter på stulna datorer. City Council i den skotska staden Glasgow blev 2012 bestulet på två bärbara datorer som innehöll information om 17.692 företag och 20.143 personer (invånare som får vinterbränslestöd och vårdbidrag). För 6.069 av invånarna fanns bankkontoinformation på de stulna datorerna.[87]

25 miljoner människor på tappad skiva. Brittiska myndigheter förlorade år 2007 en CD-skiva med personuppgifter om 25 miljoner medborgare. Den försvann i posten. Skivan innehöll bland annat födelsedatum, adress, bankkonto och nationellt försäkringsnummer vilket föranledde oro för att informationen skulle användas för identitetsstölder.[88]

Jätteläckor på Deutsche Telekom. I en insidesattack 2011 blev Deutsche Telekom bestulet på information om en halv miljon kunder. Och år 2006 tappade företaget bort en lagringsenhet som innehöll personuppgifter om 17 miljoner kunder – dessa blev sedan utbjudna till försäljning på internet.[89]

C. Buggar i systemen

Tekniska fel i ett system kan göra att skyddet plötsligt inte fungerar. Många gånger har det hänt att känslig information under en begränsad tid varit helt eller delvis tillgänglig för obehöriga på grund av fel i programvaror. Här följer några exempel.

Parkeringar avslöjade. Ett fel i systemet hos det svenska företaget Easypark gjorde att vem som helst under en tid år 2012 hade möjlighet att få reda på var människor hade parkerat sin bil. Omkring 300.000 parkerare kan vara drabbade.[90]

Tågpassagerare exponerade. Under flera veckor år 2012 var personliga uppgifter om en miljon kunder till det belgiska tågföretaget SNCB Europe tillgängliga för obehöriga via internet.[91]

Facebook läckte. Facebook har flera gånger läckt information på grund av buggar i systemen. Sommaren 2013 erkände företaget en läcka som drabbat 6 miljoner användare. Under ett års tid kunde obehöriga komma åt användarnas e-post och telefonnummer. År 2011 läckte så kallade applikationer (småprogram) på Facebook användares personuppgifter till obehöriga.[92]

Många skatteparadis läckte. Under 2013 sammanställde organisationen ”Consortium för Investigative Journalists” i Washington ett antal läckor från så kallade skatteparadis runtom i världen. Det framgår inte hur läckorna gått till. Organisationen har fått tillgång till 2,5 miljoner läckta datafiler från mer än 120.000 så kallade offshoreföretag.[93]

Svaghet i smart TV. År 2012 hittades som nämnts en teknisk svaghet i Samsungs serie teveapparater ’Smart Hub’, vilket gjorde det möjligt för hackare att aktivera tevens kamera och mikrofon och därmed lyssna/titta in i människors vardagsrum.[94]

Bugg i dokumentdelning. En bugg hos dokumentdelningstjänsten Dropbox gjorde så att under några timmar kunde vem som helst logga in på vilken användares konto som helst med vilket lösenord som helst. Obehöriga kunde därmed komma åt samtliga dokument för samtliga Dropbox- kunder. Detta skedde 2011.[95]

Slutsats:
Man kan konstatera att det enda sättet att garantera att känsliga data inte läcker är att över huvud taget inte samla in dem.

8. Hur kan man skydda sig?

Efter att ha tagit del av den mångfald av risker som finns i IT-världen uppstår den naturliga frågan: Hur skyddar man sig? Tyvärr finns inte ett enkelt och självklart svar på den frågan, men det finns många åtgärder man kan vidta som minskar risken att drabbas av problem.

Först måste man konstatera att 'säkerhet' inte är att införa maximala skyddsåtgärder – säkerhet är istället att väga de olika risker som finns mot det besvär och de kostnader som följer med olika åtgärder. På grundval av den analysen gör man sedan rimliga kompromisser. Säkerhetsåtgärder har ju så gott som alltid en kostnad, antingen i form av pengar eller i form av besvär. Vad som är en rimlig kompromiss varierar från människa till människa och från företag till företag, eftersom förutsättningarna är olika. Det kan också variera över tiden.

Rimligt är att börja med att åtgärda de mest uppenbara säkerhetsbristerna. Ingen kedja är starkare än den svagaste länken, och det är ingen idé att ha pansardörr på villan om fönsterhakarna är helt oskyddade, för att ta till en liknelse. Därefter kan man gå vidare och stärka sitt skydd, i mån av att man anser det vara värt kostnaderna. Exempel på ”low hanging fruit” när det gäller IT-skydd är god lösenordshygien och att se till att programvaror för skydd mot virus, trojaner och annan skadlig kod är installerade och uppdaterade.

Mycket beror på vilka slags risker man främst vill skydda sig mot. Nätfiskare och andra kriminella? Riktade hackerangrepp från någon som vill åt just dig? Personer i din närhet som kan vilja dig illa? Arbetsgivaren? Industrispioner? FRA och NSA? Möjligheterna att skydda sig är mycket olika beroende på vilka hot man ser som primära. Åtgärderna skiljer sig också åt.

Några saker att tänka på: Skydd av stillastående (lagrad) information är inte detsamma som skydd av information i rörelse (kommunikation). Skydd mot stöld/förlust av lagringsenhet är inte samma sak som skydd mot risker som inte bygger på stöld/förlust. Skydd mot externa angrepp är inte detsamma som skydd mot interna/närstående hot. Skydd mot hot som letar offer på måfå är inte samma sak som skydd mot hot som riktas specifikt mot dig. Skydd mot amatörer är inte samma sak som skydd mot IT-kunniga förövare. Skydd mot FRA, NSA och liknande inrättningar står i en klass för sig.

Vilka hot vill du främst skydda dig mot? Dina åtgärder blir i högsta grad beroende av svaret på den frågan. Säkerhet är ingen enkel vetenskap, och det är intressant att notera att skyddsåtgärder till och med kan bli kontraproduktiva. Om ett företag inför oerhört komplicerade säkerhetsrutiner för åtkomst till datasystemen finns risken att personalen skapar genvägar som lämnar systemen helt oskyddade. Och om man installerar en amerikansk programvara för att skydda sig mot intrång kanske man i själva verket öppnar dörren till sin dator för informationsanalytikerna på NSA.

Nedan följer en genomgång av tänkbara åtgärder för att minska risken att drabbas av intrång, avlyssning, virus, datastöld, IT-baserade bedrägerier och liknande. I nästa kapitel

kommer en lista på programvaror och tjänster som syftar till att ge IT-säkerhet.

Använd inloggning

Ställ in din dator och mobiltelefon så de kräver lösenord varje gång de startas, liksom efter en tids vila.

Tillämpa god lösenordshygien

En annan fundamental åtgärd i IT-skydd är att tillämpa god lösenordshygien. Här följer några grundläggande regler om hur lösenord väljs och används. En mera komplett lista finns här.[96] Och här[97] har Microsoft en sida där du kan testa ett lösenord och få det betygsatt (för den misstänksamma kan jag nämna att det finns de som betraktar den tjänsten som NSA:s funktion för lösenordsinsamling).

- Använd inte samma lösenord i olika sammanhang, åtminstone inte för viktiga saker.
- Använd inte för lätta eller för korta lösenord. Använd inte lösenord som utgör vanliga ord eller namn, inte ens med siffror efter, eftersom lösenordsknäckande programvaror har listor på ord och namn. Använd absolut inte ditt barns eller husdjurs namn eller något annat med koppling till dig själv. Stoppa helst in ett par specialtecken som ! och $. Ett lösenord som ”stockholm123” är svagt.
- Tänk på hur lösenordet förvaras. Framför allt, förvara det inte tillsammans med dator/mobil. Skicka det inte med e-post. Var mycket restriktiv med att lämna ut lösenordet, och byt efteråt om du måste göra det.

- Ett knep för att komma ihåg sitt lösenord är att skapa en ramsa. Lösenordet JtMgBäSoSm$ kan kommas ihåg med ”Jag tycker min gula bil är snabb och säker men dyr”, om man också kommer ihåg att göra varannan bokstav stor.
- Byt lösenord då och då. Hur ofta beror på vilken säkerhetsnivå som är nödvändig – det kanske är rimligt att byta lösenordet till banken oftare än lösenordet till en tidning på nätet.
- Låt inte webbläsare eller mobiltelefon komma ihåg lösenord.

Uppdatera skyddande programvaror

Se till att alltid ha en aktuell version av antivirusprogram (inklusive skydd mot spionprogram och annan skadlig kod). Observera att det även gäller mobilen, om du har en så kallad smartphone (vilket de flesta har). Använd brandvägg. Se också till att du har de senaste versionerna av alla ”vanliga” programvaror, eftersom säkerhetshål upptäcks ibland och då täpps till i en ny version.

Ställ in webbläsaren, och surfa smartare

Här följer några exempel på hur du kan surfa på ett säkrare sätt, både genom aktiva åtgärder och genom en lämplig inställning av webläsare.

Rensa historik. En bra åtgärd är att rensa webbläsarens historik efter varje surftillfälle. En möjlighet är förstås att surfa i privat

läge, varvid historiken inte sparas alls. I båda fall är det förstås bara de lokala spåren, i den egna datorn, som elimineras.

Neka onödiga kakor. En annan åtgärd är att vara restriktiv med vilka kakor (”cookies”) du låter webbläsaren lagra på din hårddisk, eftersom kakor kan användas för att spåra dina aktiviteter på nätet. Om du helt stänger av användningen av kakor kommer många sajter inte att fungera fullt ut, och du kanske finner åtgärden alltför kostsam i termer av besvär. Ett mellanting är att ställa in webbläsaren på att fråga om lov varje gång den tänker lagra en kaka – då kan du exempelvis neka kakor när du besöker webbsidor där du vill vara anonym. Ytterligare en tänkbar inställning är att neka så kallade tredjepartskakor. Kakinställningen brukar finnas under Säkerhet, Sekretess eller Integritet i webbläsarens inställningar.

Kolla https. När du är uppkopplad mot banker och liknande tjänster där hög säkerhet krävs ska webbadressen börja med https (ett s sist, alltså) och det ska finnas ett litet hänglås längst ned på sidan. Det visar att förbindelsen är krypterad (men NSA har knäckt den krypteringen). Det förekommer falska sajter som utgör kopior av exempelvis bankers sajter, men bara syftar till att stjäla inloggningsuppgifter, kortnummer och liknande.

Logga ut. För maximal säkerhet bör du logga ut från exempelvis Facebook och webbmejl innan du besöker andra sajter eller gör sökningar. Att förbli inloggad är en säkerhetsrisk.

Surfa via anonymisering. Om du vill surfa anonymt, och besöka sajter utan att sajtens ägare ser ditt IP-nummer (inter-

netadress), kan du surfa via en anonymiseringstjänst. Graden av säkerhet beror på vilken tjänst/programvara du använder och vilket hot du vill skydda dig mot.

Hantera e-post klokt

Det finns ett antal saker att tänka på som minskar risken för att via e-post råka ut för skadlig kod, nätfiske, datastöld eller andra problem. Här följer några råd:

- Lämna inte ut inloggningsuppgifter, lösenord, kortnummer och liknande på begäran från ett e- postmeddelande. Banker och liknande institutioner ber aldrig om sådan information via e-post (och inte heller via telefon).
- Du kan kontrollera äktheten i ett e-postmeddelande genom att ringa det företag som skickat mejlet (och då ska du förstås inte använda det eventuella telefonnummer som står i mejlet).
- Klicka inte på bilagor i e-postmeddelanden från okända, det kan initiera installering av skadlig kod på din dator.
- Tänk på att ett e-postmeddelande som ser ut att vara från en av dina vänner kan vara från en bedragare. Det finns skadlig kod som tar hela adressboken på en dator och skickar mejl till alla med begäran om någon åtgärd som syftar till att berika bedragaren. Var misstänksam, exempelvis om en vän via e-post ber att få låna pengar.
- Betrakta e-post som vykort. Skriv ingen känslig information i ett e-postmeddelande. Detsamma gäller förstås chattande och direktmeddelanden i sociala nätverk.
- Det finns många kostnadsfria tjänster som gör det möjligt att skicka e-post via en mellanhand så att din

e-postadress döljs för mottagaren. Detta kan göras på olika sätt med olika grad av säkerhet. Den engelska termen för denna slags tjänst är ”remailer”.

Var försiktig med surfzoner

Trådlösa nätverk på allmänna platser, så kallade surfzoner, utgör en säkerhetsrisk. Det finns två potentiella kategorier avlyssnare: de som satt upp nätverket och de andra personerna som är närvarande.

- Man bör inte koppla upp sig mot en surfzon med okänd upphovsman. Den som driver nätverket har stora möjligheter att avlyssna trafiken, och det kan vara ett elakt nätverk vars hela syfte är att samla in känslig information. Tänk på att en bedragare kan välja ett namn på nätverket som inger förtroende.
- Nätverk utan kryptering utgör en stor säkerhetsrisk. Vem som helst som befinner sig i samma område kan avlyssna din trafik via luften. En bedragare behöver inte ens vara närvarande – någon av de andra personerna som är uppkopplad mot samma nätverk kan ha fått sin dator smittad av ett virus som samlar in dina kontokortsnummer, lösenord och andra känsliga uppgifter.
- Ett riktigt no-no är alltså att ansluta sig till ett trådlöst nätverk som är både okänt och okrypterat. Det utgör en riktigt stor säkerhetsrisk.
- Det är ofta säkrare att ställa in sin mobiltelefon som en accesspunkt och låta datorn ansluta sig till den än att använda en publik surfzon.

- Undvik generellt att göra känsliga saker, såsom att logga in på din bank eller mata in kontokortsnummer, via en surfzon. Om du ändå måste göra det så se till att den webbplats du är inne på har en adress som börjar med https istället för http – då är trafiken som sagt krypterad.
- Stäng av funktionen ”Delning” på din dator, annars kan det vara möjligt för andra personer som är anslutna till samma surfzon att komma åt filer som är lagrade på din hårddisk.
- God säkerhet mot avlyssning vid användning av trådlösa nätverk kan uppnås genom att använda sig av en VPN-tjänst (som krypterar kommunikationen).

Skydda dig på Facebook

Här följer några åtgärder som minskar risken för att via Facebook bli utsatt för olika former av digital skada:

- Acceptera bara vänförfrågningar från personer du verkligen känner.
- Ställ in integritetsinställningarna så att du inte delar med dig information på ett bredare sätt än du verkligen anser vara nödvändigt.
- Logga ut från Facebook så snart du inte använder tjänsten. Det räcker inte att stänga fliken eller ens hela webbläsaren.
- Var misstänksam om det kommer uppmaningar att klicka på meddelanden och länkar från en vän. Skadlig kod kan ha tagit över din väns konto.
- Var misstänksam när du installerar appar/program.

- Om du är inloggad på Facebook och ändå 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 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.
- Kontrollera att Facebook är inställt på att kryptera kommunikationen med protokollet https.
- En annan säkerhetsåtgärd som Facebook tillhandahåller är engångslösenord som skickas till din mobiltelefon. Dessa är särskilt bra när man använder någon annans dator.
- Du kan också ställa in Facebook så att du får ett meddelande med e-post eller sms ifall någon loggar in på ditt konto med en annan enhet än den du brukar använda. Funktionen gör det också möjligt att avsluta den oväntade inloggningen.

Använd kryptering

Det finns olika typer av kryptering:

- Med en programvara kan hela eller delar av en hårddisk krypteras. Då är innehållet skyddat även om datorn stjäls (eventuellt lösenordsskydd av datorer kan ju kommas runt genom att helt enkelt ta ut hårddisken). Kryptering ger dock inte något absolut skydd, graden av säkerhet beror på typ av kryptering och vem man försöker skydda sig mot.

- Det finns också programvara för att kryptera sin e-post.
- Om man besöker en webbplats med en adress som börjar med https (istället för http) så använder man som nämnts krypterad kommunikation.
- Du kan kryptera din kommunikation (surfande, e-postande och annan internetkommunikation) genom att använda en så kallad VPN-tjänst.

Skydda även mobiltelefonen

Här följer några tips om vad man kan göra för att öka skyddet på mobiltelefoner (vilket ofta är försummat).

- Ställ in telefonen så den inte kan användas utan att mata in lösenord.
- Installera en säkerhetsprogramvara som skyddar mot virus och annan skadlig kod även på din mobil, inte bara på datorn.
- Installera programvara som gör det möjligt att på distans låsa telefonen eller radera dess innehåll ifall den blir stulen (funktionen ingår ofta i ovan nämnda typ av programvara). Om du har en iPhone kan detta göras med en tjänst som tillhandahålls av Apple och kan aktiveras i ”Inställningar”.
- Lämna inte telefonen obevakad när andra människor är i närheten.
- Tänk på att bilder du tar med mobilen och sedan lägger ut på nätet kan innehålla geografisk information om var bilden togs, vilket kan avslöja dina förflyttningar och din aktuella uppehållsort. Facebook tar dock automatiskt

bort sådana metadata. Du kan stänga av geotaggning, som det kallas, i din mobiltelefon.

- Appar utgör den vanligaste vägen för skadlig kod in i mobiltelefoner. Många appar skickar som nämnts personliga data om dig till sin ”ägare”. Var försiktig när du installerar appar, och bedöm om utvecklaren verkar vara trovärdig och seriös. Appar kan exempelvis skicka iväg telefonens unika ID-nummer, din geografiska position och hela din adressbok.[98] Till och med en simpel ficklampsapp kan stjäla data. En app kan innehålla ett fullfjädrat spionprogram. Om du använder en Android-telefon kan du under installationen av en app se på installationsskärmen vilka data den får tillgång till. Använder du en iPhone kan du bestämma vilka appar som ska få tillgång till din geografiska position.
- Den som vill veta mer om mobilt skydd kan läsa dokumentet ”Privacy in the Age of the Smartphone” som har publicerats av Privacy Rights Clearinghouse.[99]

Övrigt

Varning för gratisprogram. Tänk på att många gratisprogram i tysthet hämtar information från användaren och skickar till företaget bakom programvaran. Dessa är alltså, eller gränsar till, spionprogram i förklädnad. De kan också vara virussmittade.

Risker med molnet. Innan du lägger data i det så kallade molnet (”cloud computing”), betänk riskerna med detta. Din information ligger lagrad hos en avlägsen aktör, och du är i händerna på dennas säkerhetstänkande (och moral). Dina

data färdas också över internet till och från molnaktören. Särskilt tveksam till att lagra data i molnet bör man vara om man har känslig teknisk, affärsmässig eller politisk information med ett internationellt värde (NSA-varning!).

Säker radering. Tänk på att vanlig radering av en fil inte innebär att informationen tas bort. Den ligger kvar, utan att det syns för en ”vanlig” användare, och området i minnet markeras som fritt att skriva över. Säker radering måste göras med en särskild programvara som skriver över den gamla informationen med ny nonsensinformation.

När datorn kasseras. Om du säljer eller kastar bort din dator (eller mobiltelefon), tänk på att den förmodligen är fylld med känslig information om du inte genomför säker radering.

USB-minnen. Använd inte ett USB-minne som du har hittat någonstans. Det kan installera skadlig kod på din dator. Det har förekommit att avsiktligt smittade USB-minnen har planterats på platser där personer som arbetar med känslig information ofta rör sig.

9. Guide till bombsäker surfning

Trots att det finns mängder med verktyg för att skydda sig och anonymisera sin verksamhet i den digitala världen är det väldigt svårt att bli säker på att man är skyddad mot alla försök till intrång, avlyssning och registrering. Men det kan gå. Låt mig ta surfande som exempel. Så här skulle jag gå tillväga om jag ville besöka en webbplats under total anonymitet:

1. Jag skulle inte våga förlita mig enbart på en tjänst för anonymt surfande.
2. Jag skulle inte använda min egen dator eller telefon, eller en dator/telefon som har någon form av koppling till mig.
3. Istället skulle jag gå till ett bibliotek, internetcafé eller annan offentlig plats där internetupppkopplade datorer tillhandahålls utan krav på identifiering. För att skapa ett extra skyddslager skulle jag där surfa via en anonymiseringstjänst. Intressant att notera är att vissa länder har förbjudit anonymt surfande i offentliga miljöer.
4. Jag skulle låta bli att betala eventuell avgift för datorerna med kontokort eller något annat betalningsmedel som har någon som helst koppling till mig. Kontanter är däremot säkert.

5. Medan jag surfar skulle jag inte göra något som skapar en koppling till mig själv. Det innebär exempelvis att jag inte kan logga in på min Facebook, betala någonting med kort eller PayPal, boka en resa eller läsa min e-post. Undantag från förbudet att använda e-post föreligger dock om det rör sig om ett webbaserat e-postkonto som är skapat under garanterat anonym surfning och som bara används under garanterat anonym surfning, och att jag konsekvent avstår från mejlkontakt med e-postadresser som kan kopplas till mig (såsom vänner).
6. Om jag exempelvis skulle vilja starta en blogg för att driva anonym opinionsbildning kan jag inte välja en som begär att jag lämnar mitt mobilnummer (eller en e-postadress om den har minsta koppling till mig) för att sända mig ett tillfälligt lösenord.

De ovan nämnda åtgärderna torde skydda min anonymitet mot alla normala motståndare, om uttrycket tillåts. Men om jag vore Edward Snowden eller Usama bin Laden (medan han levde) räcker åtgärderna inte till. För att skydda sig mot ett högprioriterat intresse från, låt oss säga, en samarbetskoalition bestående av NSA och dess partner FRA måste man tillämpa en försiktighet som i sanning är extrem. Till de ovan nämnda åtgärderna skulle jag addera dessa:

7. Lämna mobilen hemma. Det sägs att NSA har utvecklat en metodik för att spåra mobiltelefoner även när de är avstängda.[100] Det sägs också att FBI kan aktivera en mobiltelefons mikrofon och avlyssna dess omgivningar även när den är avstängd.[101] Borttaget batteri verkar dock vara ett fungerande motmedel.

8. Se till att det inte finns någon form av registrering av min närvaro i den aktuella lokalen, alltså ingen identifierande inträdesavgift eller liknande. Detta gör exempelvis att hotellrum inte kan användas.
9. Inte använda transportmedel som registrerar min resa på ett sådant sätt att det verkar sannolikt att jag har besökt den aktuella lokalen vid den aktuella tidpunkten. Risk kan exempelvis finnas vid användning av digitala resekort för kollektivtrafiken liksom vid användning av bil. Kameror med automatisk nummerplåtsinläsning finns som nämnts på vissa håll i stadsmiljön.
10. Övervakningskameror utgör en fara för min anonymitet. Inför mitt superanonyma surfande skulle jag därför vidta långtgående åtgärder för att förändra mitt utseende, särskilt avseende ansiktet. Lösskägg, mustasch, stora glasögon, schal och peruk kan tillsammans kraftigt försvåra identifiering via kamerabilder. Om jag vore kvinna skulle jag naturligtvis ändå satsa på skägget och anta skepnad som man. Allra bäst vore att klä sig i burka (oavsett kön).
11. Man måste tänka på att det går att följa en persons förflyttningar genom en stad från övervakningskamera till övervakningskamera. Därför är det viktigt att ta på sig förklädnaden på ett ställe där detta inte kan registreras, och där det inte går att koppla samman den ”nya” personens uppdykande med den ”gamla” personens försvinnande. Beakta även spionsatelliters existens.
12. Beträffande försiktighetsåtgärderna avseende bruk av mobiltelefon bör nämnas att användning av så kallat anonymt kontantkort inte utan vidare innebär att man är anonym. Det finns flera sätt på vilka en mäktig motståndare kan koppla ett ”anonymt” kontantkort till en viss person. Det

går dock att upprätthålla en total anonymitet, åtminstone i Sverige (en del länder har förbjudit anonyma kontaktkort), men det kräver ett antal åtgärder som resulterar i en lika lång lista som denna.

13. Det är faktiskt möjligt att identifiera en person via hennes sätt att använda tangentbordet. Det är rytmen i hanteringen av tangenterna som är unik för varje människa. Även om det känns långsökt till och med för NSA att lyckas med att jämföra rytmen i tangentbordsanvändningen under besöket på biblioteket (eller motsvarande) med ett stort antal människors rytm vid deras normala surfande (när de är identifierade, såsom i hemmet) så skulle min säkerhet öka om rytmen förställs under det anonyma surfandet. Detta skulle exempelvis kunna ske genom att bara använda vänster hand (gäller högerhänta).
14. Hur är det med DNA? Den mäktiga motståndarkoalition som jag här använder som utgångspunkt för resonemanget skulle nog kunna identifiera den enskilda dator som har använts för surfandet. Datorn kommer att undersökas minutiöst. Kan agenterna avslöja mig via mina DNA- spår? Jag är ingen DNA-expert, men mot bakgrund av att det rör sig om en dator som används av väldigt många människor föreställer jag mig att DNA-spåren är sammanblandade och därför obrukbara. För maximal säkerhet anbefalls dock gummihandskar, munskydd och hårskydd. Återigen ger alltså burka en fördel. För övrigt aktualiserar resonemanget vilken stor integritetsrisk ett nationellt DNA-register skulle innebära (det krävs ju något att matcha den hittade DNA- informationen med).

Jag *tror* att dessa åtgärder skulle göra det omöjligt att koppla min person till det aktuella surfandet, till och med för världens mäktigaste motståndares prioriterade intresse. Men om man rör sig på den nivån krävs ett ständigt upprätthållande av extrema försiktighetsåtgärder. Det är oerhört lätt gjort att förr eller senare missa en länk i den nödvändiga kedjan av säkerhetsåtgärder, och en enda miss kan vara tillräckligt för att motståndaren ska bryta igenom anonymiseringen. Betänk hur Paula Broadwells lilla misstag att använda hotellrum fick henne på fall (beskrivs i avsnittet Återidentifiering och mönsterigenkänning).

För den som vill veta mer: Organisationen Privacy Rights Clearinghouse har publicerat ett stort antal faktablad om integritetsskydd för olika former av digitala aktiviteter.[102]

Appendix 1: Exempel på skyddande programvaror och tjänster

Här följer exempel på programvaror och tjänster som i skrivande stund finns tillgängliga för att skydda sin användning av datorer och mobiler. Jag har inte haft möjlighet att genomföra någon utvärdering, och kan därför inte gå i god för kvaliteten. Vissa är gratis, andra kommersiella produkter. Några överlappar varandra. Ingen värdering ligger i ordningen. Vid urvalet har privatanvändares behov, snarare än företags, legat i fokus.

Det är viktigt att ha klart för sig att graden av skydd varierar mellan de olika tjänsterna. När valet görs bör man beakta vilken typ av hot/motståndare man vill skydda sig mot, och vilka uppoffringar i form av besvär man kan acceptera. Att skydda sig mot sin sambo eller mot virus kräver inte samma åtgärder som om man vill skydda sig mot organiserad brottslighet, vilket i sin tur inte ställer samma krav som om det är NSA man uppfattar som hotet.

Man bör utgå från att säkerhetsprodukter och säkerhetstjänster, inte bara amerikanska, kan vara försedda med bakdörrar. Det enda sättet att förvissa sig om att en programvara saknar bakdörr är att utgå ifrån öppen källkod, läsa igenom hela koden och sedan kompilera den själv. Detta är tyvärr

orealistiskt för de flesta människor. Man bör också tänka på att gratisprogram ofta innehåller spionliknande funktionalitet – det förekommer att de ”ringer hem” vilket innebär att vissa data om användaren i tysthet sänds över till programmets utgivare.

Skydd mot virus, spionprogram med mera

- F-Secure Internet Security 2013
- Norton Internet Security
- Microsoft Security Essentials
- Kaspersky Internet Security
- McAfee (har flera produkter)
- Comodo
- Panda Cloud Antivirus
- Online-Armor
- MacKeeper
- Avira Free Antivirus

Brandväggar

- ZoneAlarm
- Comodo
- Online-Armor
- Private Firewall
- McAfee Next Generation Firewall
- Norton Internet Security

Anonymt och/eller krypterat surfande

- Integrity
- Relakks
- Dold
- Anonymizer

- Tor browser
- Ipredator
- Flashback
- VPNtunnel
- Anonine
- Hide My Ass
- AnonyMouse
- Safe IP
- Steganos (har produkter i flera skyddskategorier)

Tillägg till webbläsare

Det finns integritets- och säkerhetshöjande tillägg, så kallade plug-ins, till de kända webbläsarna. Dessa ger ett bättre skydd än det som finns inbyggt i webbläsarna från början. Bland de funktioner tilläggen har kan nämnas att motverka sajters och annonsörers försök till spårning av användarens surfning, att blockera scripts (som kan vara farliga), att betygsätta länkar ur säkerhetssynpunkt innan man klickar på dem, att blockera annonser och att automatiskt aktivera https-förbindelse när det är möjligt. Några sådana tillägg är:

- Ghostery – för Firefox, Chrome och Internet Explorer
- Adblock Plus – för Firefox, Chrome, Opera
- Web of Trust – för Firefox, Chrome, Internet Explorer, Safari
- Disconnect – för Firefox, Chrome, Internet Explorer, Safari
- DoNotTrackMe – för Firefox, Chrome, Internet Explorer, Safari - NoScript – för Firefox
- Https Everywhere – för Firefox och Chrome Anonym e-post, kryptering av e-post

Anonym e-post, kryptering av e-post

- Hushmail
- Countermail
- SilentSender
- AnonyMouse
- Waste project
- 10 Minute Mail
- Send Email
- Tor Mail
- CenturionSoft
- PGP
- Symantec Desktop Email Encryption
- GnuPG
- Poosty

Kryptering av hårddisk eller vissa filer

- TrueCrypt
- McAfee Endpoint Encryption
- Symantec Drive Encryption
- BitLocker Drive Encryption
- NetLib
- CheckPoint Full Disc Encryption
- PC Encrypt

Säker radering

- Eraser
- CCleaner
- PreventRestore
- FileShredder
- Darik's Boot And Nuke

Skydd för mobiltelefoner

- F-Secure Mobile Security
- BullGuard Mobile Security
- Lookout Premium
- McAfee Mobile Security
- Kaspersky Mobile Security
- ESET Mobile Security
- Trend Micro Mobile Security

Övrigt

- *Anonyma betalningar.* SpendOn är ett betalkort som fungerar som ett Mastercard, men är anonymt. Kan köpas på Pressbyrån och 7-Eleven. Här bör även Bitcoin nämnas, en digital valuta med anonyma transaktioner som dock bara kan användas på ett fåtal platser.[103]
- *Facebook-skydd*. Ökat skydd på Facebook erbjuds av Norton via Facebook Privacy Protection.
- *Säkra sökmotorer.* Det finns integritetsinriktade sökmotorer som inte placerar ut kakor på användarnas datorer och säger sig inte logga deras IP-nummer. Dessutom är uppkopplingen krypterad med https. Tre sådana sökmotorer är DuckDuck Go, Startpage och Ixquick.

NSA-säkra alternativ?

Den svenska tidskriften PC för alla publicerade i juni 2013 en lista på hur man kan ersätta olika internettjänster som kan misstänkas vara utsatta för NSA:s spionage med så kallade ”NSA-säkra alternativ”. De byten som föreslås i artikeln[104] är dessa:

Microsoft Office	-> Libre Office
Chrome, Internet Explorer, Safari	-> Firefox
Windows och OS X	-> Linux
Google Maps	-> Open Street Maps
Instagram	-> Vine
Android, IOS och WP	-> Firefox OS (ej släppt ännu)
Dropbox, Skydrive etc	-> Owncloud
Google Sök	-> Duckduckgo
Gmail, Outlook etc	-> Bitmessage
Sociala nätverk	-> Diaspora
Skype	-> Jitsi

En betydligt längre lista har publicerats på den engelskspråkiga webbplatsen Prism-Break.[105]

Appendix 2: Källförteckning

I många fall hänvisas till artiklar i tidningar och tidskrifter. Du kan enkelt hitta dessa genom att googla respektive artikels rubrik.

1 Artikel ”Avancerad IBM-lösning driver polisens romregister”, Computer Sweden, 23 september 2013
2 http://www.flexispy.com/
3 http://mobile-spy.com/
4 Artikel ”Privacy Scandal: NSA Can Spy on Smart Phone Data”, Der Spiegel, 7 september 2013
5 Trafikverkets rapport, sidan 12: http://publikationswebbutik.vv.se/upload/6984/2013_044_FOI_Trafikmatning_2012_Slutrapport_.pdf,
6 ”Polisen får se trängselskattbilder”, DN, 28 juli 2011
7 Trafikverkets rapport, sidan 19: http://publikationswebbutik.vv.se/upload/6984/2013_044_FOI_Trafikmatning_2012_Slutrapport_.pdf
8 Artikel ”Nederländerna planerar grön vägskatt”, Svenska Dagbladet, 14 november 2009, artikel ”New Pay-as-You-Go Tax for Dutch Drivers”, Der Spiegel, 16 november 2009
9 Uppslagsordet ”Vehicle miles traveled tax” på engelskspråkiga Wikipedia
10 Artikel ”Ledare: Varning för GPS-övervakning”, Expressen-GT, 12 okt 2012
11 Artikel ”Fartkamerorna ska registrera alla fordon”, Teknikens Värld, 31 maj 2011
12 Sida ”Vägledning för elektroniska nycklar”, Datainspektionen, 7 november 2007
13 Artikel ”This Is How Facebook Is Tracking Your Internet Activity”, Business Insider, 9 september 2012
14 Artikel ”This Is How Facebook Is Tracking Your Internet Activity”, Business Insider, 9 september 2012

15 Artikel ”Facebook Keeps A History Of Everyone Who Has Ever Poked You, Along With A Lot Of Other Data”, Forbes, 27 september 2011
16 Artikel ”Google’s iPhone Tracking”, Wall Street Journal, 17 februari 2012
17 Artikel ”Race Is On to ’Fingerprint’ Phones, PCs”, Wall Street Journal, 30 november 2010
18 https://panopticlick.eff.org
19 Artikel ”Can Skype eavesdrop on calls, ask privacy advocates”, Global Post, 25 januari 2013
20 Artikel ”Skype with care – Microsoft is reading everything you write”, The H Security (Heise Online), 14 maj 2013
21 Artikel ”How To Opt Out of Receiving Facebook Ads Based on Your Real-Life Shopping Activity”, Electronic Frontier Foundation, 7 mars 2013
22 https://www.eff.org/pages/reader-privacy-chart-2012
23 Artikel ”Mobilen smygkopierar kreditkortet”, Ny Teknik, 29 april 2013
24 https://dataskydd.net/overvakning-via-elmatare/ samt Datainspektionens tidskrift Integritet i fokus nr 1-2012, sidan 2
25 Artikel ”’Rifle’ Sniffs Out Vulnerability in Bluetooth Devices”, NPR, 13 april 2005
26 Artikel ”Credit card data can be stolen with a wave and an app”, CBS News, 24 april 2013, artikel ”Mobilen smygkopierar kreditkortet”, Ny Teknik, 29 april 2013
27 Artikel ”Allt fler polisanmäls för dataintrång”, Vårdförbundet, 3 april 2013
28 Notis ”Data Retention Effectively Changes the Behavior of Citizens in Germany”, Kreativrauschen.com, 4 juni 2008
29 Artikel ”Man spionerade på flickor via webbkamera”, Hufvudstadsbladet, 15 maj 2013, och artikel ”Män spionerar på unga kvinnor via webbkamera”, Hufvudstadsbladet, 17 mars 2013
30 Artikel ”Samsung TVs Can Be Hacked to Spy on Viewers”, Infowars, 14 dec 2012, artikel ”Security Hole in Samsung Smart TVs Could Let Hackers Spy On You”, Betabeat, 13 december 2012
31 Artikel ”Intel’s new TV box to point creepy spy camera at YOUR FACE”, The Register, 13 februari 2013, samt artikel ”TVs may soon be used to spy on you”, Smart Planet, 30 mars 2012
32 Artikel ”Verizon Wants to Track Your Movements While You Watch TV”, Mashable.com, 9 dec 2012
33 Artikel ”Kinect for Xbox One: An always-on, works-in-the-dark camera and microphone. What could possibly go wrong?”, ExtremeTech, 22 maj 2013
34 Artikel ”Court limits in-car FBI spying”, SecurityFocus, 19 november 2003
35 http://www1.american.edu/ted/dataprivacy.htm
36 Artikel ”The CIA wants to spy on you through your TV: Agency director says it will ’transform’ surveillance”, Daily Mail, 16 mars 2012
37 https://www.eff.org/issues/printers

38 Artikel ”FRA töjer på reglerna för sitt arbete”, Dagens Nyheter, 9 sep 2013
39 Artikel ”Spy agencies ban Lenovo PCs on security concerns”, Financial Review, 27 juli 2013
40 Artikel ”Varning: Din smarta telefon kan röja hemligheter”, Ny Teknik, 11 januari 2013
41 http://blogs.wsj.com/wtk-mobile/
42 Artikel ”Mobile location data ’present anonymity risk’ ”, BBC, 25 mars 2013
43 Artikel ”Paula Broadwell’s big mistake”, Salon, 16 nov 2012
44 Artikel ”Ditch your personal phones, use govt hardware for state secrets instead, French ministers told”, ZDnet, 12 september 2013
45 Artikel ”Brasilien vill slå till mot it-företagen”, Svenska Dagbladet Näringsliv, 13 september 2013
46 Artikel ”How Snowden got the NSA documents”, ZDnet, 26 aug 2013
47 Bloggpost på Washington Posts blogg Wonkblog ”About 500,000 private contractors have access to top- secret info” den 11 juni 2013
48 Artikel ”The secret life of J Edgar Hoover”, Guardian, 1 januari 2012
49 http://www.cunda.de/rfid, detta är bara ett exempel
50 Artikel ”Credit card data can be stolen with a wave and an app”, CBS News, 24 april 2013, artikel ”Mobilen smygkopierar kreditkortet”, Ny Teknik, 29 april 2013
51 Patentansökan ”Identification and tracking of persons using RFID-tagged items” på http://www.spychips.com/ documents/ATT00075.pdf
52 Artikel ”What if Your Boss Tracked Your Sleep, Diet, and Exercise?”, Wired, 17 april 2013.
53 http://memoto.com/
54 Artikel ”Lagförslag leder till angiverisamhälle”, Computer Sweden, 2 september 2013
55 http://www.duncancampbell.org/
56 http://www.privacyrights.org/data-breach
57 Podcast ”Bankernas mörkläggning måste stoppas”, Computer Sweden, 16 maj 2013
58 Artikel ”Dålig IT-säkerhet inom offentlig sektor”, Dagens Nyheter, 28 augusti 2013
59 Artikel ”Personuppgifter har stulits i åratal”, DN den 20 september 2012, och artikel ”Svartholm Warg: Min dator har kapats”, Expressen 20 maj 2013, artikel ”Svartholm Warg dömd till fängelse”, Dagens Nyheter, 20 juni 2013.
60 Artikel ”Svartholm Warg misstänkt för nytt intrång i Danmark”, IDG, 6 juni 2013
61 Artikel ”Vodafone Germany hack hits two million customers”, BBC, 12 september 2013
62 Artikel ”Twitter Hack Hits 250,000 Users”, PCMag.com, 1 februari 2013

63 Artikel ”Dataläcka förmörkar Iphone-lansering”, Svenska Dagbladet, 5 september 2012
64 Artikel ”Sony-vd ber om ursäkt efter intrång”, Veckans Affärer, 6 maj 2011, och artikel ”Ännu ett dataintrång mot Sony”, Svenska Dagbladet, 3 maj 2011
65 Artikel ”Dataintrång på bibliotek”, Nya Wermlands-Tidningen, 24 juni 2011
66 Artikel ”Anonymous hackade regionen - patientuppgifter kan ha läckt”, Sveriges Radio, 23 november 2012
67 Artikel ”Monster.com varnar för dataläcka”, IDG.se, 27 januari 2009
68 Artikel ”Citi Credit Card Hack Bigger Than Originally Disclosed”, Wired, 16 juni 2011
69 Artikel ”Dataläcka kostar Heartland 100 miljoner”, IDG, 13 maj 2009, samt uppslagsordet ”Albert Gonzalez” på engelskspråkiga Wikipedia
70 Artikel ”Fine for boy who hacked into Pentagon”, Independent, 22 mars 1997
71 Artikel ”15-Year-Old Admits Hacking NASA Computers”, ABC News, samt uppslagsordet ”Jonathan James” på engelskspråkiga Wikipedia.
72 Uppslagsord ”Gary McKinnon” på engelskspråkiga Wikipedia
73 Artikel ”The World from Berlin: Telekom Spying Accusations ’an Enormous Scandal’ ”, Der Spiegel, 26 maj 2008, och artikel ”Deutsche Telekom Spy Scandal: Testimony by Ex-Security Chief Piles Pressure on Former Managers”, Der Spiegel, 31 maj 2008
74 Artikel ”Kvinnojoursdator glömdes kvar i butik”, Metro, 28 augusti 2013
75 Artikel ”Anställda prickas för dataintrång på Försäkringskassan”, Folkbladet, 2 juli 2013
76 Artikel ”Socionom misstänks för 20-tal dataintrång”, Skånskan, 24 juni 2013
77 Artikel ”Bohuslänsk polis dömd för dataintrång”, Bohuslänningen, 5 februari 2013
78 Artikel ”Läkare anmäld för dataintrång”, IT i vården, 16 maj 2013
79 Artikel ”Vårdchef polisanmäld för dataintrång”, Corren, 29 maj 2013
80 Artikel ”Läkare dömd för dataintrång”, Länstidningen, 11 december 2012
81 Artikel ”Läkare åtalas för dataintrång”, Dagens Medicin, 16 oktober 2012
82 Artikel ”Läkare snokade i rivalens gynjournal”, Aftonbladet, 3 juni 2011
83 Artikel ”Läkare kan ha lämnat ut kvinnors journaler”, Expressen, 18 april 2013
84 Artikel ”Utredning om dataintrång tas upp igen”, Tidningen Vision, 26 juni 2013
85 Artikel ”A Face Is Exposed for AOL Searcher No. 4417749”, New York Times, 9 augusti 2006, samt uppslagsordet ”AOL search data leak” på engelskspråkiga Wikipedia.
86 Artikel ”Eircom laptop theft: 7,000 customers’ bank details at risk”, Silicon Republic, 10 februari 2012
87 Artikel ”Glasgow City Council fined £150,000 for loss of unencrypted laptops”, BBC, 6 juni 2013

88 Artikel ”Lost in the post - 25 million at risk after data discs go missing”, 21 november 2007, Guardian
89 Artikel ”Massive 500.000+ USB Data Breach Records Rocks Mobile Giant”, Blockmaster Security, 15 juni 2011, samt artikel ”Deutsche Telekom tystade ned stor dataläcka”, IDG, 8 oktober 2008
90 Artikel ”Dataläcka hos Easypark kan ha drabbat 300.000”, Dagens Nyheter, 14 februari 2012
91 Artikel ”Major data leak at the Belgium railway company”, European Digital Rights Association, 16 januari 2013
92 Artikel ””Facebook admits year-long data breach exposed 6 million users”, Reuters.com, 21 juni 2013, artikel ”Facebook-pudel efter dataläcka”, Dagens Nyheter, 4 november 2010
93 Artikel ”Secret Files Expose Offshore’s Global Impact”, International Consortium of Investigative Journalism, 3 april 2013
94 Artikel ”Samsung TVs Can Be Hacked to Spy on Viewers”, Infowars, 14 dec 2012
95 Artikel ”Dropbox-bugg öppnade för intrång”, idg.se, 22 juni 2011
96 https://www.privacyrights.org/ar/alertstrongpasswords.htm
97 https://www.microsoft.com/security/pc-security/password-checker.aspx
98 http://blogs.wsj.com/wtk-mobile/
99 https://www.privacyrights.org/fs/fs2b-cellprivacy.htm
100 Artikel ”NSA growth fueled by need to target terrorists”, Washington Post, 22 juli 2013
101 Bloggpost ”Can You Hear Me Now?” på bloggen ”Investigative” som tillhör ABC News, den 5 dec 2006
102 https://www.privacyrights.org/Privacy-Rights-Fact-Sheets
103 http://bitcoin.org/en/
104 Artikel ”11 sätt att undvika NSA:s spionerier”, PC för alla, 19 juni 2013
105 https://prism-break.org/

Utgivet av Den Nya Välfärden

Vadå privatliv? – Om det framväxande övervaktningssamhället (2013)
Den övermodiga beskyddaren – hur välfärdsstaten underminerar det civila samhället och urholkar dygderna (2012)
Skatteprocessen – vad varje företagare bör veta (2012)
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

En dag börjar Eva få dessa fasansfulla mejl från någon okänd person som i detalj redogör för vad hon har gjort dagen innan. Han eller hon verkar ha koll på Evas privatliv in i minsta detalj. Men vem är denna digistalker? Är det hennes ex, är det den där hantverkaren hon blivit ovän med, eller kanske de där kriminella typerna hon skrivit om i sitt jobb som journalist? Evas liv blir snabbt ett helvete och hon börjar brytas ned psykiskt.

Denna bok inleds med scenariot om Eva, och sedan förs ett resonemang om övervakningssamhället: Var de elektroniska fotspåren uppstår, hur databaser läcker, hur man kan skydda sig och vilka nya integritetsrisker som väntar i framtiden. Varför har integritetsfrågan dött i svensk debatt? Och hur påverkas människor, samhälle och näringsliv av amerikanska NSA:s spionage på världen?

den nya välfärden

Den Nya Välfärden är en opinionsbildande tankesmedja som arbetar för demokrati, välfärd och företagande. Den är partipolitiskt obunden. Läs mer på: www.dnv.se

PRIS: 79 KR

ISBN 978-91-977488-5-8