

.SE Nyhetsbrev om Internets styrning september 2013

[Blogg:](#)

.se

1

[Nyhetsbrev:](#)

Internetutvecklingen styrs idag endast i begränsad utsträckning av samma aktörer som för fem eller tio år sedan. Anspråken på hur nätet ska styras kommer från flera håll samtidigt. Det är en komplex uppgift bara att överblicka alla försök till styrning av nätets utveckling.

På .SE vill vi med detta brev bidra till omvärldsbevakningen av denna process. Brevet kommer månadsvis. Sammanställningen gäller utvecklingen i Sverige, EU och globalt, och fokuserar i första hand på händelser som rör Internets styrning och hoten mot det öppna Internet. Brevets innehåll är en kortfattad inventering och pekare mot aktuella frågor. Tematiska fördjupningar, kommentarer och åsikter ligger i bilaga. Ibland ligger åsikter också i halvårssummeringar.

Innehåll

Förenta nationerna	4
FN:s generalförsamling	4
ICANN	4
ICANN om delegering och återtagande av landstoppdomäner	4
Villkor för tillväxt, handel och kommersiella förutsättningar	4
Googles eventuella dominerande ställning i Europa	4
Integritet online	5
OECD reviderar guidelines för privacy	5
Facebooks nya integritetspolicy	5
Yahoo släpper Transparency report	5
Internationell ranking av digitala rätigheter	5
Internet som Infrastruktur	5
Google	5
EU-kommissionens förslag till reglering av telefoni och Internetaccess	6
Men bidrar regelverket till nätneutralitet?	6
Ett europeiskt e-ID - igen	7
Blandade rapporter	8
ENISA säkerhetsrapport	8
Ett lokalt IGF i Norge	8
ISOC-NO ger råd	8
Finlands UD berättar om TTIP	8
Finsk forskning om hur övervakning påverkar vårt beteende	8
Ett lokalt Internet Governance Forum i Norge	8
Sacharovpriset till Snowden?	8
Internetdagarna 2013	9
Ny generaldirektör för FRA	9
Statsbudgeten – för informationssamhället	9
Svensk behandling av Europarådets konvention om IT-realterad brottslighet	9
Bilaga: Efter Snowden – del 3	12
Avlyssning i Mexico, Brasilien och Indien:	13

Förfalskade elektroniska certifikat	14
Knäckt och avsiktligt försvagad Internetkryptering	14
Effekterna:	15
BRIC-länderna vill lämna USA:s hegemoni över Internet	15
Symptom på eftertanke och legala reformer i USA	15
Brittisk utredning om effekterna av Snowdens avslöjanden	15
Europaparlamentets rapport om PRISM och FISA	16
Företagen reagerar	16
Sveriges roll:	16
Mer att läsa	17
Bilaga 2 - Svensk tillsyn av svensk Internetavlyssning - Siun.....	18
Granskaren	18
Skydd av individens integritet?	18
Kryphål?	19
Slutsatsen.....	19

Kommentarer, synpunkter eller frågor:

Staffan Jonson, .SE (Stiftelsen för Internetinfrastruktur), Box 7399, 103 91 STOCKHOLM,
tel 073-317 39 67, Staffan.jonson@iis.se , www.iis.se

Globalt

Även i september har alla nyheter rörande Internets styrning överskuggats av det globala system för Internetövervakning som uppdagats i sviterna efter Edward Snowdens avslöjanden. I bilaga finns en tredje sammanfattning av läget.

Förenta nationerna

FN:s generalförsamling

I FN:s generalförsamling uppmärksammades avslöjandena om amerikansk Internetavlyssning (se vidare bilaga). Särskilt Brasiliens president Dilma Rousseff höll ett eldfängt tal som i mycket starka ordalag kritiserade USA:s agerande när det gäller Internetavlyssning. Känga efter känga delades ut, t.ex. följande.

"In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. In the absence of the respect for sovereignty, there is no basis for the relationship among nations."

Det kanske mest olyckliga för Internetkramare världen över var emellertid det förnyade bränsle för internationell Internetreglering som nu blev ett krav i generalförsamlingen. Guardian rapporterar hur Rousseff begärde att FN ska leda ett nytt globalt regelverk för styrningen av Internet. Hon efterlyste en FN-reglering som ska tillförsäkra rätten till yttrandefrihet samt skyddet av individens integritet och mänskliga rättigheter.¹

ICANN

ICANN om delegering och återtagande av landstopptomäner

ICANN Remitterar under september utkast till policy för redelegering och ev. återtagande av landstopptomäner (delegation and redelegation of ccTLD). Svar senast 30 september.²

Villkor för tillväxt, handel och kommersiella förutsättningar

Googles eventuella dominerande ställning i Europa

Google har lämnat in 'concessions till EU-kommissionen i hopp om att undvika böter på 5 Miljarder US\$. Som tidigare rapporterats håller EU-kommissionen sedan tre år tillbaka på att granska Googles eventuella missbruk av sin dominerande ställning i Europa när det gäller sökningar på nätet.³

¹ <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance> och <http://gadebate.un.org> och <http://gadebate.un.org/68/brazil>

² <http://www.icann.org/en/news/public-comment/cctld-drd-ui-policy-09sep13-en.htm>
<http://www.ntia.doc.gov/page/iana-functions-purchase-order>

³ http://news.cnet.com/8301-1023_3-57601968-93/in-eu-antitrust-case-google-ratchets-ups-concessions/
http://hosted.ap.org/dynamic/stories/E/EU_EUROPE_GOOGLE_ANTITRUST?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT

Integritet online

OECD reviderar guidelines för privacy

OECD har reviderat sina Guidelines för Privacy. Det var på huvudkontoret i Paris som man beslutade om *revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.⁴

Facebooks nya integritetspolicy

Facebook har nyligen släppt en ny integritetspolicy. Den amerikanska tillsynsmyndigheten (Federal Trade Commission, FTC) meddelar att den inlett en granskning om Facebook därmed bryter en överenskommelse från 2011. Enligt den snart två år gamla överenskommelsen ska företaget få uttrycklig accept från en användare innan de publicerar hennes privata uppgifter till en ny publik.⁵

Yahoo släpper Transparency report

Även Yahoo sällade sig i september till den rad av amerikanska IT-företag som lämnar en s.k. Transparency report, dvs. rapporter om hur många förfrågningar om användardata som kommit från rättsvårdande myndigheter.

<http://bits.blogs.nytimes.com/2013/09/06/yahoo-releases-first-government-transparency-report/>

Internationell ranking av digitala rättigheter

New America Foundation gör digitala rättigheter mätbara genom ett rprojekt kallat Ranking Digital Rights. Projektet syftar till att utveckla en metod för att mäta och rangordna internationella IT-bolag då det gäller deras verksamhets respekt för yttrandefrihet och personlig integritet.⁶

Internet som Infrastruktur

Google

En av de mer konkreta effekterna av Snowdens avslöjanden är Google initiativ till förnyade tekniker att kryptera innehållet på företagets servrar. Åtgärden har givetvis inte en allomfattande effekt, men sägs åtminstone försvåra avlyssningen.⁷

⁴ <http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines>

⁵ <http://www.nytimes.com/2013/09/12/technology/personaltech/ftc-looking-into-facebook-privacy-policy.html>

⁶ <http://rankingdigitalrights.org> och <http://newamerica.net/node/91553>

⁷ http://news.cnet.com/8301-1023_3-57601820-93/google-accelerates-encryption-project/

http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html

Europa

EU-kommissionens förslag till reglering av telefoni och Internetaccess

<https://ec.europa.eu/digital-agenda/en/news/regulation-european-parliament-and-council-laying-down-measures-concerning-european-single>

Som rapporterats tidigare meddelade EU-kommissionen under våren om ytterligare ett nytt förslag till reglering av marknaderna för telefoni- och Internetaccess. Under september konkretiserades förslaget, och blev offentligt.

Målsättningen är att genom att fullända den inre marknaden för mobila datatjänster ska en europeisk konkurrenskraft stärkas. Förslaget har som bekant hos konsumenterna 'sålts in' till en bredare europeisk allmänhet genom löfte om avskaffade roamingavgifter och därmed troligtvis i praktiken enhetstaxa inom EU.

En av de mer kontroversiella målen är behovet av att konsolidera den europeiska mobilmarknaden, dvs. där finns en förhoppning om att minska antalet operatörer från över tusen idag, till en handfull.

När man borrar något djupare i reaktionerna är det många institutioner som uttrycker tydligt missnöje med förslagen. Den generella kritiken handlar om att förslaget forceras genom institutionerna, så att Europaparlamentet ska beslut att anta förslaget inom nuvarande mandatperiod, dvs. innan valet i maj 2014.

Det europeiska samarbetsorganet för 28 regulatorers samarbete (BEREC) formulerade i september ett ovanligt explicit muttrande över förslagen. Bland annat avfärdades de just som forcerade. Särskilt riktade BEREC spetsen mot den nya bärande tanken i policyn att konsolidera antalet operatörer.

BEREC uttryckte vidare oro över en ändrad maktbalans mellan centraliserad EU-politik i Bryssel å ena sidan, och nationella regulatorer, å andra sidan. Man hade också velat bli inbjudna att delta i planeringen av förslaget redan från början.⁸

Telekombranschen är inte heller helt lycklig över förslaget. ETNO har anlitat Strand Reports att berätta att europeisk mobilindustri kommer att kollapsa, samt att arbetslösheten i Europa kommer att öka ifall förslaget genomförs. En enhetlig inre marknad för elektronisk mobil kommunikation sågas också av Boston Consulting Group.⁹

Men bidrar regelverket till nätneutralitet?

Nellie Kroes har tydligt argumenterat för att hennes nya Europeiska regelverk ska bidra till nätneutralitet. Hennes argumentation bygger på att eftersom endast Nederländerna och Slovenien har explicita Nätneutralitetslagar, skulle 96% av Unionens befolkning sakna sådan lagstiftning.

Särskilt Telekomoperatörerna tycks tagna på sängen av den nya viljan att konsolidera de europeiska marknaderna för telefoni/Internetaccess (ISP:er). En bärande tanke om att minska antalet europeiska ISP:er från över tusen till en handfull, har seglat upp till favoritplats hos Kroes.

⁸ http://bereg.europa.eu/eng/news_consultations/whats_new/1598-berec-statement-on-the-publication-of-a-european-commission-proposal-for-a-regulation-on-the-european-single-market

⁹ http://www.etno.be/datas/publications/studies/BCG_ETNO_REPORT_2013.pdf
<http://www.strandreports.com/sw5671.asp>

Men utifrån målet om nätneutralitet kritiseras den s.k. Artikel 23 i förslaget som kontraproduktiv. Kritiker menar att förslaget bidrar till ett icke neutralt nät. I nuvarande utkast säger artikel 23 att föreslagen lag ska hindra Internetleverantörer från att blockera eller bromsa Internet-trafik: "*blocking, slowing down, degrading or discriminating against specific content, applications or services.*"

Kritiker menar emellertid att artikel 23 öppnar för prisdifferentierad Internetaccess (s.k. two tiered Internet). Formuleringen i Artikel 23 om definierad kvalitet i tjänsterna ("*specialized services with a defined quality of service or dedicated capacity.*") kan också tas som intäkt för prisdifferentierade tjänstekvalitet.

Kroes å sin sida menar att denna risk inte är överhängande eftersom artikeln också har en generell formulering om kvaliteten i Internetaccess (att sådana tjänster inte "... shall [...] impair in a recurring or continuous manner the general quality of Internet access services,").

Enligt samma källa försvarar Kommissionens talesman Ryan Heath företagens möjlighet att (pris-) differentiera kvaliteten i Internetaccess, (dvs. en affärsmässigt motiverad inskränkning av nätneutralitet). Hans argumentation baseras på att post- och flygtjänster tillåts prisdifferentiera i decennier, varför det också vore riktigt när det gäller Internetaccess.¹⁰

Kritik av Kommissionens förslag kommer också från samvetsorganisationen Access. Samma artikel 23 står här på nytt i skottgluggen, men nu kritiseras den i stället i den otydliga avgränsningen av vad som ska menas med 'rimlig trafikstyrning'. I punkt 47 i regelverket hänfaller Kommissionen som så ofta till att det är OK att titta i Internet-trafiken ('dvs. tillämpa s.k. *deep packet inspection*' så fort någon uttalar orden "allvarliga brott" eller "barnpornografi"). Därmed förutsätter lagstiftaren återigen att trafikförmedlaren (ISP:er m.fl.) ska ägna sig åt att bedriva polisarbete i näten. Lagstiftaren förutsätter också att formuleringar om 'gott omdöme' och 'goda avsikter' ska räcka för att filtrera Internets innehåll till en rimlig balans mellan brottsbekämpning och frihet på nätet.¹¹

Ett europeiskt e-ID - igen

Även processen med ett nytt europeiskt eID har gått långt. Det nya regelverket syftar till:

- att ersätta befintligt e-signaturdirektiv
- att kräva ömsesidigt erkännande mellan *nationella e-ID-system*.
- att skapa ett legalt ramverk för förtroendetjänster

10 december planeras Parlamentet rösta om en Europa-övergripande reglering av elektroniska identitetstjänster. I likhet med exempelvis NIS-direktivet finns det för utomstående ett behov av förtydligande av exakt vad regleringen avser, och ett förtydligande av hur implementeringen ska gå till.

Rapportör i Parlamentet är Marita Ulvskog, skuggad av Pilar del Castillo, Jürgen Creutzmann, Amelia Andersdotter och Sajjad Karim.¹²

¹⁰ <http://www.pcworld.com/article/2048563/digital-rights-activist-eus-proposed-net-neutrality-law-as-useful-as-an-umbrella-in-a-hurricane.html>
<https://www.laquadrature.net/en/pcworld-digital-rights-activist-eus-proposed-net-neutrality-law-as-useful-as-an-umbrella-in-a-hurric>

¹¹ <https://www.accessnow.org/blog/2013/09/17/commission-proposal-fails-to-deliver-promise-of-net-neutrality>

¹² <http://goo.gl/SdeyK1>

Blandade rapporter

ENISA säkerhetsrapport

Den europeiska Nätverkssäkerhetsmyndigheten ENISA har publicerat en ny rapport. En av rapportens slutsatser är att SPAM minskar för andra året i rad.¹³

Ett lokalt IGF i Norge

Norska PT håller 9 oktober ett s.k. Nationellt Internet Governance Forum i Oslo.¹⁴

ISOC-NO ger råd

Nymornade *ISOC Norway Chapter* är tidigt ute med råd till den nya norska regeringen. Den norska regeringen uppmanas ta en stadig dialog med den amerikanska regeringen om NSA:s globala system för Internetavlyssning.¹⁵

Finlands UD berättar om TTIP

I Finland höll utrikesministeriet i september ett möte för att informera en intresserad allmänhet om handelsavtalet TTIP. Mötet syftar till att ge en överblick av förhandlingarna, och av vilka mål Finland har för mötet.¹⁶

Finsk forskning om hur övervakning påverkar vårt beteende

I Helsingfors har det genomförts ett långvarigt experiment om hur allorstädes närvarande övervakning i hemmet påverkar människor.¹⁷

Ett lokalt Internet Governance Forum i Norge

Ett lokalt Internet Governance Forum hålls i Oslo 9 oktober. Dagen efter hålls ett nätneutralitetsforum.¹⁸

Sacharovpriset till Snowden?

Det har under september pågått en kampanj för att få EU-parlamentet att nominera Edward Snowden som årets vinnare av [Sacharov-priset](#).

¹³ <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013/>

¹⁴ <http://www.npt.no/aktuelt/nyheter/nasjonalt-internet-governance-forum-2013>

¹⁵ <http://ikt-norge.no/2013/09/lykke-til-med-forhandlingene-i-nydalen-etterpa-ma-dere-forhandle-med-nsa/>

¹⁶ <http://formin.finland.fi/public/default.aspx?contentid=283363&nodeid=15145&contentlan=2&culture=en-US>

¹⁷ <http://hpe.hiit.fi/p41-oulasvirta.pdf>

http://www.svd.se/kultur/overvakningen-forandrar-oss_8528274.svd

¹⁸ <http://www.npt.no/aktuelt/nyheter/pt-inviterer-til-nettnøytralitetsforum-2013>

<http://www.npt.no/aktuelt/nyheter/programmet-for-nasjonalt-internet-governance-forum-er-klart>

Sverige

Internetdagarna 2013

Internetkonferensen Internetdagarna går i år av stapeln 25-26 november, på Waterfront i Stockholm. Nytt för i år är att konferensen sker genom ett uttryckligt flerpartssamarbete, dvs. flera parallella konferenser under ett tak. Biljettpriset har sänkts betydligt, jämför med tidigare år, till 1250 kr per dag, men förutsätter därmed ett begränsat tillträde till en konferens per dag.

Ny generaldirektör för FRA

Regeringen utsåg i september Dag Hartelius till ny generaldirektör för FRA.¹⁹

Statsbudgeten – för informationssamhället

Årets statsbudget inbegriper satsningar på bredbandsutbyggnad, en effektivisering av offentlig förvaltning, samt en inventering - och därmed effektivare användning av – offentligt ägd IT-infrastruktur.

Nytt i IT-politiken för effektivisering av offentlig förvaltning är ett s.k. *flerårigt utvecklingsprogram*. Det kan liknas vid en ökad kameral flexibilitet i myndigheternas möjligheter att investera i IT-system som ger kostnadsbesparingar först flera år senare. Konkret kan sådant uppnås genom utökad låneram för myndigheterna, och att den ramen görs flerårig i statsbudgeten.²⁰

Svensk behandling av Europarådets konvention om IT-relaterad brottslighet

Justitiedepartementet har haft betänkandet rörande *Europarådets konvention om IT-relaterad brottslighet* (SOU 2013:39) ute på remiss.²¹

Utredningen har haft tre ändamål:

- att analysera behovet av och lämna förslag till de författningsändringar som krävs för att Sverige ska kunna tillträda Europarådets konvention om IT-relaterad brottslighet och dess tilläggsprotokoll.
- att analysera behovet av och lämna förslag till de författningsändringar som behövs för att genomföra Europaparlamentets och rådets kommande men ännu inte formellt antagna direktiv om angrepp mot informationssystem och om ersättande av rambeslut 2005/222/RIF.
- att överväga behovet av skärpta straff för brytande av post- eller telehemlighet och dataintrång för att ge ett ökat utrymme att på ett nyanserat sätt beakta allvaret i storskaliga angrepp mot informations- system.

Computer Sweden har skrivit en översiktlig sammanfattning om kritiken mot lagförslaget. Det har där snabbt döpts till "Angiverilag".²²

Flera instanser avstyrker förslagen:

¹⁹ <http://www.regeringen.se/sb/d/17017/a/223461>

²⁰ <http://www.regeringen.se/sb/d/2373/a/16433>

²¹ diarienummer Ju2013/4173/Å och *Europarådets konvention om IT-relaterad brottslighet* (SOU 2013:39).

²² <http://computersweden.idg.se/2.2683/1.525015/tunga-instanser-sagar-angiverilag>

Advokatsamfundet avstyrker i sitt remissvar att huvuddelen av förslagen läggs till grund för lagstiftning.²³

Internetoperatören Bahnhof är kritisk till såväl innehåll som syfte med betänkandet.²⁴ IT- och telekomföretagen är inte heller särskilt glada över förslaget. Man menar bl.a. att teknisk expertis inte tillfrågats innan förslaget lagts fram.

²³ http://www.advokatsamfundet.se/Documents/Advokatsamfundet_sv/Remissvar/440586_20130920155655.pdf

²⁴ <http://bahnhof.se/filestorage/userfiles/file/Remissvar2013-09-18.pdf>

Kalendarium

Norska PT håller 9 oktober ett s.k. Nationellt Internet Governance Forum i Oslo.
<http://www.npt.no/aktuelt/nyheter/najonalt-internet-governance-forum-2013>
[Seoul Conference on Cyberspace](#), 17-18 oktober 2013, Seoul, korea 21-25 oktober 2013,
[Internet Governance Forum](#) (IGF), 22-25 oktober, Bali, Indonesien
[RGIG](#) på PTS: 5 november kl.13-16
ICANN 48 i Buenos Aires, Argentina 17-21 november 2013
Regionala förberedelsemöten inför WTDC, november 2013
[Internetdagarna](#), Stockholm, 25-26 november 2013
[Integritetskonferens](#), 22-24 januari, 2014
ICANN 49 i Singapore våren 2014
WTDC (april 14)
WSIS-mötet efter WTDC (april 14)
Stockholm Internet Forum (SIF 14), 27-28 maj 2014
ICANN 50 i London sommar 2014
ICANN 51 i Nordamerika höst 2014
High level WSIS +10 Review, 2014 Kairo
IGF 2014,
ITU Plenipotentiary 2014, Busan, Korea
ITU:s fyraårsplaner vid PP-14
ITU:s finansiella plan vid PP-14

Ett globalt system för Internetavlyssning

Bilaga: Efter Snowden – del 3

Rapporten är en fortsättning på artikeln *Amerikanska statens program för Internetövervakning*, som ingick som bilaga till .SE nyhetsbrev för Internet i juni 2013 samt sommar (juli till augusti) 2013. En inventering av många av de uppgifter som läckts finns i Google docs: <https://t.co/P1Fne5VgAp>.²⁵

*"Too many wrongly characterize the NSA debate as security versus privacy.
The real choice is liberty versus control"*

- Bruce Schneier, @schneierblog

I slutat av augusti och september kom en 'andra våg' av avslöjanden efter Snowdens initiala avslöjanden. Den här månaden har vi bl.a. lärt oss:

- att amerikanska och brittiska underrättelsetjänsterna kan begå intrång i en betydande del av Internet-trafiken, och att de genom hot eller traditionell 'kodknäckning' forcerat sådana krypton som tidigare ansågs 'säkra' (t.ex. Internetbanker)
- att amerikanska NSA:s program för avlyssning på intet sätt är avgränsat till försvar av landet mot terrorism, och inte heller att det avgränsas till en defensiv verksamhet.
- att NSA arbetar offensivt, bl.a. med cyberattacker, kryptoknäckning och avsiktligt underminerande (försvagande) av standarder för kryptering av elektronisk kommunikation.²⁶ Det blev också klart att myndigheten även fortsättningsvis söker 'tysta ner' läckor om verksamheten.²⁷
- att avlyssningen syftar tillsådan kartläggning av sociala relationer som också uppdagades i samband med FRA-lagen (att skapa sociogram)²⁸
- att myndigheten inte bara avlyssnar EU:s kontor i FN, utan även att Mexicos och Brasiliens presidenters elektroniska kommunikation avlyssnats, samt att Brasiliens dominerande oljebolag avlyssnats, inför en förestående global auktion om rätten att utvinna nyfunnen olja i landet. Målet för avlyssningen har också varit EU:s institutioner i Belgien, och Indiens diplomatiska representationer i Washington och FN-representationen i New York.
- att avlyssningen avser mer än sjökablar och ambassader. NSA ska enligt uppgifterna satt upp team för att knäcka skyddet i vanliga mobiler.²⁹ Därmed har intrång i smarta mobiler som t.ex. iphone, Googles androidlurar eller BlackBerry kunnat ske. Särskilt Kanadensiska BlackBerry har marknadsförts som en extra säker mobil eftersom den hållit en något högre grad av kryptering. Telefonens kryptering knäcktes i mars 2010.³⁰

²⁵ Via Twitter från @mikko: Spreadsheet detailing the Surveillance leaks of 2013: <https://t.co/P1Fne5VgAp>

²⁶ <http://www.propublica.org/article/the-nasas-secret-campaign-to-crack-undermine-internet-encryption>, se vidare nedan

²⁷ <http://www.aftonbladet.se/nyheter/article17420027.ab>

²⁸ <http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html>

²⁹ <http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html>

³⁰ <http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html>

Mycket få uppgifter har dementerats.

Till och med Internet Society³¹ uttryckte för andra gången denna sommar bestörtning över rapporterna om NSA:s försök att kringgå grundläggande säkerhetsmekanismer.³² Från ordförande i *Internet Engineering Task Force* (IETF)³³ kom också tydliga reaktioner, och resonemang om hur nätet ska göras säkrare mot intrång.³⁴

Avlyssning i Mexico, Brasilien och Indien:

Det blev också klart Mexicos och Brasiliens presidenters elektroniska kommunikation avlyssnats. Brasilianska oljebolaget Petrobras har också haft påhälsning. Nyupptäckta Brasilianska oljedepåer ska snart auktioneras ut, vilket sätts i samband med avlyssning av företaget.

Den indiska ambassaden i Washington och vid FN:s permanenta representation i New York ska också ha avlyssnats.³⁵

Den Brasilianska reaktionen har inte dröjt. President Dilma Rousseff ställde in ett planerat statsbesök i USA senare i höst, och uppgifter om flera åtgärder för att lösgöra sig från *amerikansk Internet-hegemoni* har hörts.³⁶

En av åtgärderna sägs bli att brasiliansk Internet-trafik i framtiden i huvudsak ska ledas (routas) via andra länder än USA, t.ex. genom att etablera direkta sjökablar till Europa. Vidare talas det om krav på att amerikanska företag skulle tvingas drifva sina elektroniska tjänster inom Brasilien. Exempelvis Google, Facebook eller Apple skulle därmed tvingas ha sina servrar i landet, som villkor för att erbjuda tjänsterna till Brazilianare. Därmed skulle brasiliansk lag kunna tillämpas på företagens tjänster, och underförstått en bättre kontroll mot avlyssning kunna ske.

Det senare fenomenet, dvs. att via nationell lag tvinga fram en anpassning av Internetinfrastrukturen efter nationalstaternas gränser kallas ofta för en *balkanisering* av Internet. En sådan balkanisering är också det första steget mot ändrade affärsmodeller för nätet, liknande den traditionella telefonins debitering för trafikförmedling över landsgränser.

Brasiliens reaktion på USA:s Internetbaserade industrispionage riskerar med andra ord att ha långtgående effekter också för affärsmässig styrning av nätet. Det gränsöverskridande Internet är en struktur som redan idag tillgodoser viss konkurrens mellan Internetleverantörer. Om flera länder ägnar sig åt att anpassa sin Internetinfrastruktur efter nationsgränser kommer vi också snart se en protektionism i Internetaccess som gynnar lokala monopol, som höjer priserna för Internetanvändare, men som i sig i mycket begränsad utsträckning bidrar till ett säkrare Internet.

³¹ Internet Society (ISOC.org) är en organisation som är djupt rotad i amerikansk techie-kultur, och som vanligtvis är mycket försiktig i sina uttalanden.

³² <http://www.internetsociety.org/news/internet-society-responds-reports-us-government's-circumvention-encryption-technology>

³³ IETF är den organisation ...

³⁴ <http://www.ietf.org/blog/2013/09/security-and-pervasive-monitoring/>
http://www.circleid.com/posts/ietf_chairs_statement_on_security_privacy_and_widespread_internet_monitorin/

Organisationen har sin vana trogen etablerat en ny e-postlista för ändamålet: The [perpass mailing list](mailto:perpass@ietf.org) (perpass@ietf.org), en lista som särskilt diskuterar hur IETF borde reagera på uppgifterna om systematiskt avlyssning.

³⁵ <http://www.thehindu.com/news/international/world/nsa-planted-bugs-at-indian-missions-in-dc-un/article5164944.ece>

³⁶ <http://world.time.com/2013/09/18/brazil-looks-to-break-from-u-s-centric-internet/>

Internetkramare har länge varnat för att en avsaknad av affärsmässig nätneutralitet skulle kunna bidra till en sådan balkanisering. Nu riskerar den i stället uppstå som en följd av bristande förtroende.³⁷

Det amerikanska spionagets chef James R Clapper dementerade att avlyssningen av de brasilianska oljebolagen hade några andra avsikter än terrorbekämpning. Han förklarade i ett särskilt yttrande att USA inte använder information inhämtad genom sin underrättelsetjänst för att stjäla handelshemligheter från företag i andra länder, eller för att stärka amerikanska företags resultaträkningar.³⁸

Under den gångna månaden kom det också uppgifter i Der Spiegel om att brittiska GCHQ Genomfört en avsiktlig attack mot halvstatliga Belgacom. Under kodnamnet ”operation socialist” skulle målet ha varit att ”... enable better exploitation of Belgacom”. Europa-institutionerna i Bryssel är kunder hos- , och får sin Internetaccess från Belgacom.³⁹

Förfalskade elektroniska certifikat

Den amerikanske säkerhetsexperten Bruce Schneier redogjorde för hur NSA tros hackat företaget Diginotar, för att på så sätt ha förfalskat företagets certifikat. Diginotar utfärdar certifikaten för att hjälpa Internetanvändare att etablera en säker anslutning med webbläsare, och genom att förfalska dessa kan en s.k. *man-in-the-middle*-attack genomföras. En *man-in-the-middle*-attack kan användas för att dirigera Internetanvändare till en falsk websida, där exempelvis användarnamn och lösenord kapas. Den holländska regeringen använde tidigare Diginotars certifikat.

Knäckt och avsiktligt försvagad Internetkryptering

Under sommaren lärde vi oss också att NSA ska ha knäckt s.k. säkra krypteringar, dvs. exempelvis sådan kryptering som används av Internetbanker. Enligt journalistsajten Propublica ska detta varit del i en systematisk kampanj för att hindra alltför effektiv kryptering. Det talas exempelvis om *bakdörrar* i kryptostandarder, om systematisk avlyssning av [SSL-protokollet](#), om intrång i [VPN-tunnlar](#), med mera. Enligt samma källa pågår den kampanjen fortfarande.⁴⁰

³⁷ <http://www.reuters.com/article/2013/09/08/us-usa-security-snowden-petrobras-idUSBRE9870AD20130908?irpc=932>
<http://www.dn.se/nyheter/varlden/nya-uppgifter-om-usa-spionage-mot-brasilien/>
<http://www.startribune.com/politics/national/222023281.html>
www.theverge.com/2013/8/31/4680544/nsa-spied-on-al-jazeeras-internal-communication-system-new-leak
<http://www.institutolula.org/lula-o-presidente-dos-estados-unidos-deveria-pedir-desculpas-ao-mundo/#.Uioz--gaySO>
<http://www.techdirt.com/articles/20130917/11525924555/more-nsa-spying-fallout-brazilian-president-cancels-visit-to-us-starts-internet-balkanization.shtml>
http://www.washingtonpost.com/world/europe/experts-see-potential-perils-in-brazil-push-to-break-with-us-centric-internet-over-nsa-spying/2013/09/17/c9093f32-1f4e-11e3-9ad0-96244100e647_story.html
http://www.washingtonpost.com/world/europe/experts-see-potential-perils-in-brazil-push-to-break-with-us-centric-internet-over-nsa-spying/2013/09/17/c9093f32-1f4e-11e3-9ad0-96244100e647_story.html

³⁸ <http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence>

³⁹ <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html>

⁴⁰ <http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>

<http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>

<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

BBC *ibid*: <http://www.bbc.co.uk/news/world-us-canada-23981291>

CS inventerar:

<http://computersweden.idg.se/2.2683/1.521352/nya-lackan---det-har-vet-vi>

<http://www.dn.se/ekonomi/teknik/usa-har-knackt-sakra-krypteringar/>

<http://arstechnica.com/security/2013/09/nsas-pipe-dream-weakening-crypto-will-only-help-the-good-guys/#p3>

<http://edition.cnn.com/2013/09/06/us/nsa-surveillance-encryption/index.html>

<http://m.democracynow.org/stories/13873>

Vidare finns en hypotes lanserad av the Times och New York Times om att NSA åtminstone sedan 2006 arbetat med att avsiktligt underminerar Internetkrypteringens kvalitet, bland annat i den internationella standardiseringsorganisation N.I.S.T, med 163 länder som medlemmar. I [Wired](#)⁴¹ utvecklas den hypotesen.⁴²

Effekterna:

BRIC-länderna vill lämna USA:s hegemoni över Internet

Som beskrevs ovan vill Brasilien 'ta sig ur USA:s hegemoni över Internet', främst genom åtgärder och investeringar i Internetinfrastrukturen. Den viljan är inte en isolerad händelse, utan något vi troligtvis kommer att se mer av.

Enligt inte bekräftat e-post-skvaller kommer BRIC-länderna på ITU-konferensen 2014 avisera att de lämnar den USA-baserade DNS-roten. Den uppgiften bör rimligtvis tas med en nypa salt, men den representerar åtminstone en grad av indignation som inte är vanlig.⁴³

Symptom på eftertanke och legala reformer i USA

Det börjar också komma symptom på eftertanke i sviterna av Snowden. Avslöjandena har öppnat ögonen för en inhemsk amerikansk debatt. Lagförslag som ska begränsa NSA:s befogenhet att övervaka nätet har presenterats. I *the Intelligence Oversight and Surveillance Reform Act* finns exempelvis initiativ till att hindra den systematiska insamlingen av telefoni-uppgifter. Initiativet innebär också att det ska finnas en *constitutional advocat*, dvs. något som troligtvis kan liknas vid en ombudsman för privacy-frågor.⁴⁴

I Samband med Obamas Stockholmsbesök nämnde han möjligheten att begränsa NSA:s makt. Han medgav på presskonferensen att det finns rimliga skäl ("legitimate questions") att ifrågasätta NSA:s roll. Amerikanska kongressledamöter har tidigare krävt lagändring för att begränsa NSA:s makt. Enligt Guardian är det första gången Obama också öppnar för den möjligheten.⁴⁵

I Washington har den första utredningen kring NSA-avslöjandena snart deadline för redovisning. Utredarnas självständiga roll ifrågasätts emellertid.⁴⁶

Brittisk utredning om effekterna av Snowdens avslöjanden

Även Storbritanniens *information commissioner*, Christopher Graham beställde under sommaren en utredning om i vilken utsträckning avslöjandena om massövervakning har effekt för Internetanvändarens personliga integritet på nätet.

Särskilt fokus ska enligt The Guardian läggas på de relativt nya uppgifterna om att NSA och GCHQ ägnat sig åt att knäcka kommersiell kryptering, t.ex. sådan som används i

⁴¹ <http://www.wired.com/threatlevel/2013/09/nsa-backdoor/>

⁴² <http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/>

<http://www.bbc.co.uk/news/technology-24048343>

⁴³ <http://www.thehindu.com/news/international/world/brazil-plans-to-go-offline-from-uscentric-internet/article5137689.ece>

<http://www.globalresearch.ca/the-brics-independent-internet-in-defiance-of-the-us-centric-internet/5350272#>

<http://www.excitingrio.com/brazil-looks-break-us-centric-internet/>

⁴⁴ <http://www.theguardian.com/world/2013/sep/25/nsa-reform-bill-surveillance-congress>

<http://www.theverge.com/2013/9/25/4771878/intelligence-oversight-surveillance-reform-act-constitutional-advocate>

⁴⁵ http://www.theguardian.com/world/2013/sep/04/barack-obama-nsa-powers-laws?CMP=tw_t_gu

<http://www.youtube.com/watch?v=XTMjPokoH7o>

⁴⁶ <http://bigstory.ap.org/article/close-ties-between-white-house-nsa-spying-review>

Internetbanker. Detta sedan Der Spiegel⁴⁷ publicerat uppgifter om att NSA övervakar kreditföretaget VISA:s transaktioner.⁴⁸

Europaparlamentets rapport om PRISM och FISA

20 september släppte Europaparlamentet ett första utkast av sin rapport rörande PRISM och FISA-domstolen. Rapporten tar emellertid inte upp brittiska GCHQ:s roll i avlyssningen.⁴⁹

Internetkramande organisationer som EDRI och FREE har också gjort en ambitiös juridisk analys av den påstådda avlyssningen, och en inventering av eventuella juridiska effekter. Rapporten lämnades till LIBE.⁵⁰

Företagen reagerar

Det har hittills varit svårt att genomså de stora Internetföretagens roll. I juni gav företagens ledningar och pressavdelningar intryck av att vara helt ovetande om den avlyssning som pågick. Allteftersom uppgifter läckt har de emellertid vågat ta en mer aktiv roll i att informera allmänheten. Man har särskilt uppvaktat den amerikanska staten för att slippa den munkavle man ålagts om pågående verksamhet.

I september öppnade Yahoos Marissa Mayer, och Facebooks Mark Zuckerberg munnen om företagens tidigare inkonsekventa beteenden i media. Mayer bekräftade att företagets ledning avstått från att publicera uppgifter om den pågående avlyssningen pga. rädsla för fängelsestraff.

Företagen ingår också i en tilltagande kör av bloggare som bekräftar vilken stor skada, och vilket eroderat förtroende NSA-besluten gjort för amerikanska Internetföretag.⁵¹

Sveriges roll:

Mycket av Sveriges roll i det internationella avlyssnings-samarbetet är känt redan sedan tiden för FRA-debatten.⁵² Att Sverige och FRA har en central roll i det internationella samarbetet bekräftades i september av journalisten Campbell. Det var i Europaparlamentets hearing i utskottet för medborgerliga fri- och rättigheter (LIBE) som han bekräftade att Sverige – under namnet *Sardine* – utgjort en sådan roll.⁵³

I september kom också ett uttalande från ett svenskt statsråd. Det var Försvarsminister Karin Enström som lättade på förlåten då det gäller avlyssningen. Där meddelade hon att hon förutsatte att myndigheten följer lagen, dvs. ett icke-uttalande i frågan.⁵⁴

I Sverige har också DN rapporterat om tillsynsmyndighetens Siuns kritik av FRA:s arbete.⁵⁵ Se vidare separat inlägg nedan.

⁴⁷ <http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html>

⁴⁸ <http://www.theguardian.com/world/2013/sep/19/uk-information-commissioner-snowden-disclosures>

⁴⁹ http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf
<https://publicintelligence.net/eu-nsa-surveillance/>

⁵⁰ http://www.edri.org/edri_free

⁵¹ <http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance>

⁵² <http://www.svt.se/nyheter/sverige/riksdagspartier-begar-korten-pa-bordet-om-fra>

⁵³ <http://henrikalexandersson.blogspot.be/2013/09/fra-ar-nyckelspelare-i-det-globala.html>

<http://www.europarl.europa.eu/ep-live/de/committees/video?event=20130905-0900-COMMITTEE-LIBE>

http://www.svd.se/nyheter/inrikes/sverige-deltog-i-nsa-overvakning_8492260.svd

http://www.svd.se/nyheter/inrikes/ryssland-malet-for-fra-lagen_1444077.svd

<http://www.metro.se/teknik/video-har-pekare-duncan-campbell-ut-sverige/EVHmif!DURGOGm2hJtog/>

⁵⁴ <http://www.sydsvenskan.se/sverige/forsvarsministern-om-fra/>

⁵⁵ DN:a granskning:

Revision i Sverige: SIUN säger att FRA upprepade gånger brutit mot reglerna

<http://www.dn.se/nyheter/sverige/fra-tojer-pa-reglerna-for-sitt-arbete/>

Mer att läsa

Många tyckare har givetvis vädrat synpunkter på den nya insikten om den systematiska avlyssningen. Amerikanen Bruce Schneier exempelvis, ondgör sig över hur USA *kidnappat Internet* (Commandeered the Internet).

Schneier FTC och Privacy:

https://www.schneier.com/blog/archives/2013/08/the_federal_tra.html

Schneier: USA commandeering the Internet

https://www.schneier.com/blog/archives/2013/08/more_on_the_nsa.html

Schneier: låt oss ta tillbaka Internet

<http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying>

"Too many wrongly characterize the NSA debate as #security versus #privacy. The real choice is liberty versus control," @schneierblog says

(<https://twitter.com/Liberationtech/status/377087817463386112>)

Obamas order från juni 2013 att lista mål för cyberkrigföring:

<http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text>

<http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>

USA:s avsikter

<http://www.techdirt.com/articles/20130906/09472224429/nsa-defends-encryption-breaking-promising-its-only-used-to-spy-all-us.shtml>

NSA och FISA-domstolen

<http://www.techdirt.com/articles/20130906/02305724426/nsa-didnt-actually-address-all-fisa-courts-concerns-contrary-to-what-it-claims.shtml>

Greewald om knäckt kryptering

<http://m.democracynow.org/stories/13873>

Schneier 1 https://www.schneier.com/blog/archives/2013/09/conspiracy_theo_1.html

<http://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat>

<http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance>

Schneiers survival Kit

Schneier: 1. Använd Tor <http://t.co/WietYKMCC6>

Schneier: 2. Kryptera all kommunikation <http://t.co/WietYKMCC6>

Schneier: 3. Utgå från att din dator kan vara ägd men att den antagligen inte är det <http://t.co/WietYKMCC6>

Schneier: 4. Använd inte kommersiella kryptoproducter <http://t.co/WietYKMCC6>

Schneier: 5. Använd fri programvara för kryptering <http://t.co/WietYKMCC6>

Om Keith Alexander

The Cowboy of the NSA - Inside Gen. Keith Alexander's all-out, barely-legal drive to build the ultimate spy machine

<http://t.co/WdDnl7H5Py>

[Blogg:](#)

[Nyhetsbrev:](#)

Bilaga 2 - Svensk tillsyn av svensk Internetavlyssning - Siun

Granskaren

Portalparagrafen säger:

”Statens inspektion för försvarsunderrättelseverksamheten (Siun) är den myndighet som har till uppgift att kontrollera att den försvarsunderrättelseverksamhet som bedrivs av Försvarmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut sker i enlighet med det av riksdagen och regeringen fastställda regelverket.”⁵⁶

Domstolens uppgift är mao. att tillse att aktuella myndigheter håller sig till aktuellt regelverk, dvs. traditionell tillsyn. Först i andra hand kommer omsorg om individens integritet.

”Siun ska även på enskilda begäran kontrollera om hans eller hennes meddelande har inhämtats i samband med signalspaning samt säkerställa att Försvarets radioanstalt endast ska få tillgång till de signalbärare för vilka Försvarsunderrättelsemyndigheten medgivit tillstånd”⁵⁷

Vi lär oss också att Siun är en *politisk domstol* av svenskt snitt, dvs., utöver ordförande och vice ordförande nomineras den styrande nämnden av riksdagspartierna.⁵⁸

Skydd av individens integritet?

Domstolens andra uppgift är att bistå enskilda att åtminstone i efterhand kunna granska ifall de varit avlyssnade. Vi som testat denna efterhandstillsyn upptäckte snart en viktig detalj. När jag frågar Siun ifall jag varit avlyssnad säger sig Siun visserligen granska om mina meddelanden blivit avlyssnade, *men bara baserat på de uppgifter jag lämnar till myndigheten.*

Vad innebär det? Konkret behöver jag anta att det betyder att Siun endast kontrollerar ifall den uppgift (i det här fallet namn1.namn1@gmail.com) jag lämnar till myndigheten lyssnats av, och inget annat. Siuns granskning säger inget om huruvida min andra uppgift (namn2.namn2@yahoo.com) lyssnats av. Jag frågar alltså Siun ifall jag som individ blivit avlyssnad. Men Siun svarar att e-postadressen namn1.namn1@gmail.com åtminstone inte blivit det. Jag får helt enkelt inte svar på frågan.

Annorlunda uttryckt innebär denna ordning att bevisbördan skiftats över på den som frågar. Jag som enskild behöver komma ihåg alla mina konton, och lämna in en komplett lista över dem till Siun för att få visshet i huruvida jag fått min elektroniska kommunikation avlyssnad eller inte.

Därmed tillkommer nästa frågeställning: Hur behandlar Siun den listan från en enskild? Vad säger exempelvis Datainspektionen om integriteten i en förteckning över individens samtliga elektroniska tjänster? Blir den listan en offentlig handling hos domstolen?

Siuns förmåga att ge individer svar på huruvida de blivit avlyssnade är i bästa fall svår, i praktiken närapå praktiskt ogenomförbar. Integritetsskyddet hos individen är med andra ord inte funktionellt.

Även om individer skulle skicka in långa listor på alla sina e-tjänster, så har domstolen troligtvis inte resurskapacitet att svara alla. Den aspekten av domstolens verksamhet kan inte

⁵⁶ http://www.siun.se/om_siun.html

⁵⁷ <http://www.siun.se/begaran.html> Att ett meddelande eventuellt ”... har inhämtats i samband med signalspaning” betyder här helt enkelt att exempelvis ett mejl, ett inlägg på facebook eller chat-meddelande har avlyssnats av FRA.

⁵⁸ http://www.siun.se/om_siun.html

betraktas som något annat än en kosmetiskt eftergift till riksdagen. Siuns resurser att tillhandahålla integritetsskydd till individer behöver betraktas som undermåligt.

Kryphål?

Det finns mycket att säga om avlyssningens räckvidd, men särskilt en del av lagtexten reser fler frågetecken än den ger svar:

Det finns exempelvis i lagtexten kvar en textsnutt som ger FRA möjligheten att ”..*fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag*”.⁵⁹

Texten antyder att det handlar om en tillfällig metodutveckling för att utveckla spaningen, men formuleras som ett kontinuerligt undantag. Vad som inte regleras där är exempelvis vad man gör med den data som samlas in i denna fortlöpande metodutveckling. Den är med andra ord redan i en ytlig översikt en stor möjlighet till undantag från lagens mening.

En mindre välvillig tolkning av texten skulle kunna innebära att FRA här har en frizon att spana på vem/vilka, hur, hur mycket och när man vill, dvs. den gummiparagraf som behövs ifall handlingsfriheten i de andra paragraferna täpps till. Huruvida den möjligheten används kan bara Siun avgöra.

Slutsatsen

Som framgår ovan har svensk tillsyn av både teoretiska och praktiska skäl liten förutsättning hjälpa den enskilde kunna övervaka sin egen integritet online i Sverige. Det finns också troligtvis kryphål kvar som *möjliggör* ett missbrukas.

Det har nyligen uppmärksammats att Siun i sin tillsyn lyckats belägga FRA med missbruk av sin ställning vid åtminstone nio tillfällen. Försvarsministern tar i ett uttalande nyligen dessa händelser som inteckning för att tillsynen fungerar, dvs. hon *förutsätter* att FRA ändrar sitt nuvarande beteende. Men vad händer i de nio fall där FRA belagts med missbruk? Vad händer med de nio (?) personer som då blivit otillbörligt avlyssnade? Blir de automatiskt uppmärksammade på att deras integritet på nätet felaktigt kränkts av en myndighet? Eller får de söka reda på denna information själva, genom att kanske lyckas ställa rätt fråga till domstolen?

Den övergripande frågan handlar om vad som händer ifall myndigheter inte har för avsikt att ta till sig också lagens mening, utan stannar vid dess bokstav. I amerikanska NSA:s fall har vi sett en långtgående cynism på detta område, där senatorer fått svar på sina frågor först då de vet hur frågorn ska ställas. FRA:s samarbete med främmande underrättelsetjänst smittar svenska myndigheters trovärdighet på det området.

⁵⁹ Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet, 1§ sista stycket.