Fra rådet til tinget
TEKNOLOGIRÅDETS NYHEDSBREV TIL FOLKETINGET

Nr. 186 | oktober 2003

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

IT-privacy skal forbedres

Borgernes ret til privacy i digital forvaltning kan støttes af teknologi og lovgivning

Frygt for offentlig overvågning >

Øget offentlig overvågning og registrering via bl.a. digital forvaltning kan føre til, at befolkningen mister tilliden til mulighederne i informationssamfundet. Der er teknologier og metoder på vej, som både kan effektivisere informationssamfundet og minimere risikoen for misbrug af personlige data.

Forebyg misbrug med virtuelle identiteter >

Stephan Engberg foreslår at bruge virtuelle identiteter til at give borgerne kontrol over egne data. Han kritiserer den nye sundhedsportal, som han ikke mener imødekommer borgernes behov.

Tyveri af identitet største problem >

Søren Duus Østergård fremhæver tyveri af identitet som det største privacy-problem. Edb-sproget EPAL kan være med til at forhindre ulovlig indsamling at personfølsomme data.

Offentlig efterspørgsel skal drive udvikling af PET's >

Marit Hansen advarer mod at bruge CPR-nummeret i digital identitet, fordi det øger risikoen for misbrug. Offentlige IT-projekter som digital forvaltning skal satse på privacy-forbedrende teknologier og derved skubbe til udviklingen.

Dette Fra rådet til tinget ser på de udfordringer til privacy i informationssamfundet og bud på teknologiske løsninger, specielt i tilknytning til digital forvaltning

Mængden af følsomme informationer om borgerne er hastigt stigende i informations-samfundet. Informationer om vores uddannelse, privatøkonomi, politiske tilhørsforhold, indkøbsvaner og meget andet bliver opsamlet og registreret. Vi efterlader os elektroniske spor overalt, når vi surfer på Internettet, vores mobiltelefoner afslører hvor vi befinder os, vores email-kommunikation og oplysninger om, hvem vi har talt med, lagres hos teleoperatørerne, registreringer i PBS fortæller hvor vi har handlet. Hvis informationerne kædes sammen, opstår muligheden for at misbruge dem. Og når data samles centralt på servere, der er tilgængelige via Internet, som det fx ses i den nyligt lancerede sundhedsportal, er der også større risiko for hacking og misbrug. Vi er ikke altid vidende om, at vores færden i den digitale verden registreres, eller til hvilket formål. At vi ikke selv kontrollerer, hvem der indsamler og får adgang til personlige oplysninger, hvornår og i hvilken sammenhæng, er en af de centrale udfordringer til privacy. Sikkerhed for, at vi er dem vi giver os ud for, når vi kommunikerer med andre i den digitale verden, er et andet vigtigt aspekt.
Ønsket om at opnå størst mulig sikkerhed, fx i terrorbekæmpelse, kan bruges som argument for at slække på kravene til privacy. Men det indebærer en fare for demokratiet. Hvis befolkningens frygt for registrering stiger, bliver det sværere at få folk til at bruge e-handel og digital forvaltning.
Bestyrelsen for den digitale task-force har på baggrund af anbefalinger fra en arbejdsgruppe om borgernes IT-rettigheder under Ministeriet for Videnskab, Teknologi og Udvikling, og den store opmærksomhed i EU på privacy, diskuteret emnet på deres seneste møde.
Fra rådet til tinget har talt med tre eksperter, som alle arbejder med at udvikle teknologier, der kan forbedre privacy for borgerne og samtidig sikrer, at bå-

de e-handel og digital forvaltning kan fungere. Alle tre er enige om, at truslen mod privacy er et voksende problem, men deres bud på løsninger er forskellige. Specielt ser de forskelligt på spørgsmålet om man altid skal identificere sig eller må bruge pseudonymer, når man færdes i den digitale verden.

Hvad er privacy?
Den første definition af privacy blev givet af den amerikanske højesteretsdommer Louis Brandeis i 1890'erne, som formulerede privacy som individets demokratiske "right to be left alone".
Siden er der gjort mange forsøg på at definere begrebet, som grundlæggende drejer sig om retten til at være alene uden at være overvåget af andre, og retten til at bestemme, hvad man vil offentliggøre om sig selv og under hvilke omstændigheder. Men der findes ikke èn definition.
I den digitale verden taler man ofte både om sikkerhed, beskyttelse af personfølsomme data, og om privacy som et bredere begreb relateret til den personlige integritet og selvbestemmelse. Privacy kan således omhandle at give brugerne rettigheder til fx at få oplyst, hvor deres personlige data registreres, og til at slette og ændre i de personlige data. Og det kan omhandle at give brugerne kontrol over deres data, så de bestemmer, hvem der kan tilgå dem, til hvilket formål og hvornår de må kædes sammen.
Man kan skelne mellem følgende niveauer i beskyttelse af privacy i den digitale verden:
- anonymitet, hvor identiteten ikke kan genskabes, (fx afstemning)
- pseudonymer, anonymt, men hvor man kan afgøre, at det altid er samme person, der bruger pseudonymet (fx PGP-nøgle)
- ansvarligt pseudonym, hvor identiteten kan genskabes under særligt beskyttede forhold, (fx virtuel identitet)
- identifikation, enten direkte (fx med et pas), eller gennem en ansvarlig part, (fx TDC's Digitale Signatur)

Advarer mod identifikation og registrering

Stephan Engberg, direktør i Open Business Innovation, peger på, at Danmark tidligt valgte at anvende en entydig identifikation af borgerne på tværs af alle offentlige IT-systemer, CPR-nummeret. Brugen af entydig identifikation som princip har bredt sig til stort set alle områder af samfundet. Men der stilles ikke spørgsmålstegn ved, om det altid er nødvendigt at registrere borgerne med CPR-numre i alle offentlige databaser.
I overgangen til digital forvaltning fortsætter man med at opbygge centrale og stadigt mere detaljerede "dossiers" over den enkelte borger – og som noget nyt får stadig flere systemer og institutioner adgang til oplysningerne. Det øger mulighederne for misbrug af personlige data markant, mener han. Konsekvensen kan meget vel være, at borgerne får mistillid og bliver stadig mere bange for informationssamfundet, som dermed bliver dyrere og vanskeligere at få til at hænge sammen.
Stephan Engberg nævner den nye sundhedsportal som eksempel på unødvendig registersamkøring og centralisering af adgangen til data om borgerne. Når man samler al kontakt til sundhedssektoren, herunder til EPJ, ét sted, skaber man en unødvendig sikkerhedsrisiko. De samme services kan etableres mere sikkert og trygt i en konstruktion, hvor kontrollen med data decentraliseres.

Virtuelle identiteter og signaturer

Stephan Engberg mener, at løsningen på borgernes behov for kontrol med egne data er "virtuelle identiteter" (ansvarlige pseudonymer). Han er selv primus motor i udviklingen af et privacy-koncept baseret på virtuelle identiteter – et koncept, han har indgivet patentansøgning på. Det bygger på åbne standarder og placeres ovenpå den eksisterende infrastruktur – fx telefon- og mailsystemer, digital signatur og PBS.
Grundtanken er, at den enkelte bruger ved hjælp af anonymiserings- og pseudonymiseringsteknologier bygger virtuelle identiteter ovenpå sin egen, cpr-baserede identitet. I stedet for én digital identitet bruger man mange forskellige. Det kan fx være når man handler på nettet, læser internetavis, bruger sit kreditkort i forretninger, låner bøger på biblioteket, får taget et røntgenbillede, taler i telefon og meget andet. Virtuel identitet er et forsøg på at "oversætte" de forskellige roller og dermed forskellig grad af fortrolighed og tillid, som vi til daglig veksler imellem, alt efter om vi er sammen med venner, på arbejde, ude at købe ind etc.
Pointen er, at internetbutikken, avisen, biblioteket, supermarkedet, teleselskabet osv. ikke har adgang til personens identitet, og dermed heller ikke til oplysninger, man ikke selv har valgt at give fra sig. Og det bliver ufarligt frivilligt at afgive informationer, fordi pseudonyme data ikke kan sælges og selv en hacker kan ikke misbruge dem.
Umiddelbart kan det virke besværligt at den enkelte bruger skal administrere flere virtuelle identiteter, men ifølge Stephan Engberg kan man også ved hjælp af teknologien sikre, at det hverken bliver kompliceret eller ineffektivt. Virtuel identitet vil i daglig brug kunne træde i stedet for den digitale signatur. Men Open Business Innovations koncept indebærer ikke, at man fuldstændigt undgår at identificere sig. Stephan Engberg understreger, at den digitale infrastruktur ikke kan bygge på anonymitet.
I mange situationer er der behov for at kombinere sin virtuelle identitet med sin identificerende digitale signatur. Det gælder fx overfor lægen, banken, præsten og sagsbehandleren, men ikke overfor ad-

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyhedsbreve findes på:
www.tekno.dk/rtt.htm

ministrationen eller Sundhedsportalen. Man kan bruge den grad af identifikation, der passer til situationen, men kontrollen ligger altid decentralt, hos den enkelte bruger, siger Stephan Engberg.
Han understreger, at der i hans koncept er indbygget en sikring af borgernes ansvarlighed, så der normalt ikke er behov for yderligere identifikation. Ved kriminelle handlinger er der mulighed for at koble et cpr-nummer til en virtuel identitet, men det sker via nøgler kontrolleret af eksterne parter, fx en domstol.
Ifølge Stephan Engberg fjerner hans koncept de centrale bindinger mellem effektivisering, privacy og kriminalitetsbekæmpelse og gør det til et politisk valg, hvor meget frihed individet skal have på bekostning af samfundets kontrol – og omvendt. Som udgangspunkt mener han, at man som borger aldrig bør identificeres med mindre der er en nødvendig grund til det, eller man selv ønsker det.

Tyveri af identitet største problem

Søren Duus Østergaard, Senior e-government advisor for IBM i Europa, Mellemøsten og Afrika, er enig i, at det er på høje tid at tage privacy problemet alvorligt. Men han fremstiller et andet trusselsbillede: Den største trussel mod privacy er tyveri af identitet. Hvis det lykkes at opsamle tilstrækkelig med personlige informationer via elektroniske kanaler, kan man ansøge om fx et nyt pas eller kørekort og ad den vej overtage en persons identitet. Han peger på, at identitetstyveri er blevet en af de mest almindelige typer af cyber-kriminalitet. Årsagen er, at første stop mod bl.a. illegal immigration og andre kriminelle aktiviteter over grænser er at skaffe sig en ny identitet.
På trusselslisten kommer herefter tyveri af kreditkortinformationer med efterfølgende finansielt bedrageri, brug af andres identitet til at foretage langdistance telefonopkald og lignende aktiviteter. Herefter følger trusler mod de fundamentale borgerrettigheder – fx ved at man får fat i og publicerer personlige oplysninger om en person, som skader denne. Eller personlige oplysninger som fx bruges til afpresningsformål. Det fjerde niveau er informationsindsamling om en person, som derefter misbruges i forbindelse med markedsføring eller andre informationsformål – fx i form af uønsket spammail.

EPAL - et privacy-filter

Søren Duus Østergaard og IBM er fortalere for, at ethvert individ spiller med åbne kort og identificerer sig, også i den virtuelle verden. Ellers hæmmer vi kommunikationen og det bliver sværere at udfolde informationssamfundet på en funktionsdygtig måde, mener han. Men man skal bruge teknologien til at begrænse adgangen til de personlige informationer, der opsamles i alverdens databaser. Det er muligt at lave et system, som sikrer, at køber og sælger, afsender og modtager, ved hvem hinanden er, samtidig med at de personlige informationer sikres.

Borgernes syn på privacy

Borgernes bekymringer for øget registrering og overvågning er kommet frem i en række danske og udenlandske undersøgelser. Blandt andet kan nævnes:
Teknologisk Fremsyn om Pervasive Computing,fra Ministeriet for Videnskab, Teknologi og Udvikling, 2002. Interview med en gruppe borgere, der repræsenterer et bredt udsnit af befolkningen, og en gruppe, der har et særligt teknologikendskab. Begge grupper giver udtryk for, at teknologien er ved at tage kontrollen med deres liv, og mange mener, at den tiltagende offentlige overvågning og registrering fører til en reduktion i individets personlige frihed og råderum.
www.teknologiskfremsyn.dk/html/ikt_pubs.html.

Et borgerpanel nedsat af Teknologirådet i 2002 vurderede, at elektroniske patientjournaler først og fremmest er patientens ejendom og at de får kontrollen med hvem der får adgang til deres EPJ.
http://www.tekno.dk/pdf/nummer182.pdf

Det franske The Internet Right Forum, en uafhængig gruppe af forskere og borgere, udsendte i 2003 en rapport, som kritiserer offentlige portaler med oplysninger om borgerne, fordi de administreres centralt og dermed udenfor borgernes egen kontrol.
www.foruminternet.org/en/publication/

Det engelske Prime Ministers Strategy Unit har udgivet rapporten: Privacy and Datasharing, The Way forward for Public Service. I rapportens bilag C undersøges borgernes holdninger, og her omtales bl.a. den udbredte opgivende holdning overfor især den private sektors indsamling af personlige data. Borgerne føler ikke de har kontrol eller valgmuligheder, og rapporten advarer om, at denne fatalisme kan udløse stærke modreaktioner.
http://www.number-10.gov.uk/su/privacy/annex-c.htm

IBM har udviklet et helt nyt edb-sprog, EPAL (Enterprise Privacy Architecture Language), som er målrettet til at kunne disse ting. Det er en åben, frit tilgængelig standard, som kan anvendes i relation til stort set alle internationale, standardiserede databaser, som indeholder personlige data, der skal beskyttes.
Søren Duus Østergaard betegner EPAL som et filter, der kan placeres mellem databasen og brugerne af databasen. EPAL spiller sammen med den privacy politik, som virksomheden eller organisationen har

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyhedsbreve findes på:
www.tekno.dk/rtt.htm

vedtaget, og sprogets funktion er at håndtere identitet og adgangsrettigheder for personer, der ønsker adgang til data. Den administrerer adgang til personfølsomme data udfra det samtykke, som ejeren af data har givet, og som både kan handle om hvem der må bruge data og under hvilke omstændigheder. Desuden bliver alle aktiviteter logged efter læserens identitet, formål, situation, hvis data og hvornår.
EPAL har i det seneste år været afprøvet af en global hotelkæde og af et lands sundhedssystem, og Søren Duus Østergaard oplyser, at IBM's forskningslaboratorium i Zurich har stillet EPAL til rådighed for det uafhængige konsortie bag web-standarderne. Konsortiet overvejer nu at publicere EPAL som en åben standard.

Sundhedsportal og EPJ

Sundhedsportalen, som ventes taget i brug i december, lever ikke op til borgernes krav om fuld kontrol med egne data, mener Stephan Engberg. I stedet for at lave egentlig adgangsbegrænsning til EPJ, har man valgt en model, der er opbygget som et Intranet i sundhedsvæsenet med sundhedsportalen som indgang. Han mener, at sikkerheden reelt består i, at man overvåger hvilke personer, der går ind i de enkelte elektroniske journaler, i stedet for at forebygge misbrug.
Selvom EPJ i sig selv er en kompleks problemstilling, så mener Stephan Engberg at det er muligt at opbygge kompatible EPJ-sikkerhedsmodeller, opdelt i separate afsnit, som hver kræver forskellige adgangsnøgler afhængig af hvem, der ønsker adgang. Og hvor informationerne som udgangspunkt ikke er identificerbare, fx i relation til at anvende journaloplysninger til statistiske, forskningsmæssige og administrative formål, som udgør hovedparten af brugen af sundhedsdata. De identificerende informationer krypteres særskilt og er kun tilgængelige decentralt på arbejdsstationerne for dem, der har tilgang til nøglerne på den specifikke patient. Apoteker, medicinproducenter og centrale myndigheder kan være koblet til de relevante dele af en pseudonym EPJ uden af den grund at få adgang til patientens samlede, identificerende medicinprofil eller sygdomshistorik, påpeger Stephan Engberg. Mens patienten selv og lægen kan have fuld adgang til alle EPJ-oplysninger og dermed bevare overblikket over patientens situation.
Søren Duus Østergaard fra IBM mener heller ikke, at digital signatur, som den ser ud i TDCs udgave, er tilstrækkelig til at imødekomme de sikkerhedskrav, der bør være i relation til Sundhedsportalen og EPJ. I den sammenhæng bør man kræve et såkaldt "kvalificeret certifikat", der udstedes på samme måde som et pas – det vil sige ved at man møder op personligt. TDCs digitale signatur rekvireres på baggrund af en pinkode på selvangivelsen, hvilket indebærer en for stor risiko for misbrug og falske identiteter.
Søren Duus Østergaard peger dog på, at den nuværende digitale signatur, som han betegner som et "letvægtscertifikat", udmærket kan benyttes i den del af kommunikationen med det offentlige, som ikke kræver høj sikkerhed. Dog pointerer han, at udviklingen bør gå i retning af at introducere kvalificerede certifikater. Hvad også EU anbefaler, siger han.

PET – privacy enhancing technologies:
PET kan beskrives som teknologier, der sigter mod at fjerne eller begrænse opbevaringen og udvekslingen af personlige data. Blandt andet kan anonymisering og pseudonymisering anvendes. Men der er ingen færdig definition af PET.
ICPP definerer PET bredt som: "Enhver teknologi, der som minimum lever op til lovgivning om privacy og som også forbedrer den teknologiske state-of-the-art af privacy- og databeskyttelses værktøjer".

Tyske PET's

Marit Hansen er leder af afdelingen for Privacy Enhancing Technologies (PET's) på det uafhængige center for privacy beskyttelse i Slesvig-Holsten, ICPP. Hun har beskæftiget sig indgående med sikkerhed og privacy og deltager i en række EU-projekter, som omhandler fremtidsorienterede løsninger på privacy og identitetsadministration (Identity Management) i Europa.
Marit Hansens udgangspunkt er, at de teknologier, som sikrer troværdighed og ansvarlighed mellem parterne i den digitale verden, skal udvikles til også at forbedre privacy for brugerne.
Hun finder at IBM's EPAL absolut er værd at arbejde videre med, fordi det styrker privacy funktionaliteten i eksisterende informationssystemer.
Men hun mener også, at man er nødt til at udvikle privacy-løsninger baseret på pseudonyme digitale identiteter i stil med Stephan Engbergs koncept. Brugen af pseudonymer er en god metode til at fremme privacy, fordi det minimerer mængden af personidentificerbare data. Målet må være at give brugerne kontrol over flow'et af personlige data og adgang til at bestemme, i hvor høj grad andre må kæde ens data sammen.
Marit Hansen er meget kritisk overfor den måde, vi i Danmark bruger CPR-nummeret. Og hun advarer mod at integrere CPR-nummeret i digital identitet, fordi det øger risikoen for misbrug og registersammenkøring.
Set med hendes øjne er udfordringen ved overgangen til digital forvaltning at sikre den enkeltes ret til selvbestemmelse over personlige informationer. Det nuværende niveau af privacy for brugere af offentlige serviceydelser skal fastholdes, og derfor er man nødt til at integrere sikkerheds- og privacy-forbedrende teknologier i den digitale forvaltning.
Selv arbejder hun bl.a. i et EU-projekt med at udvikle privacy-forbedrende identitets-administrations-

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

systemer (IMS). IMS bruges til sikker adgang til e-handel, internetbanker, teleselskaber, flyselskaber mm. Men det er langtfra alle IMS der udbydes i dag, der også forbedrer privacy. At udvikle disse redskaber og understøtte brugen af dem, ikke bare på brugerens side, men også i udbydersystemerne og i infrastrukturen er én strategi til at fremme privacy, siger Marit Hansen, som forventer at det tager mindst 10 år, før privacy forbedrende IMS er i distribution.

Privacy-certifikat og ombudsmand

Men teknologi gør det ikke alene. Det skal understøttes af lovgivning, som understreger den enkeltes selvbestemmelse og muligheder for at bruge pseudonymer eller forskellige digitale identiteter, siger Marit Hansen, med henvisning til tysk lovgivning, som stiller krav om, at man designer og udvælger IT-systemer med henblik på at anonymisere eller pseudonymisere menneskers identitet, så vidt det er muligt.
Hvis udviklingen af privacy-forbedrende teknologier skal fremmes, har sådanne lovkrav stor betydning. Marit Hansen peger også på, at man kan forpligte nationale projekter som fx digital forvaltning til at foretrække privacy-forbedrende teknologier.
ICPP har taget initativ til et privacy-certifikat, som udbydere af IT-produkter kan opnå. Den markedsføringsfordel det giver, har ifølge Marit Hansen øget virksomhedernes interesse for at forbedre deres produkter, så de lever op til lovkravene til beskyttelse af privacy. Idéen bliver nu taget op i en lov om Overvågning og Certificering af Privacy for hele den tyske føderation.
Stephan Engberg synes, at der er inspiration at hente i den tyske lovgivning. Men han fremhæver samtidig, at der mangler forretningsmæssige drivere i Danmark, fordi der fx i Persondatalovens samtykkebestemmelser ikke skelnes mellem pseudonyme og identificerede persondata. Det er den primære årsag til, at der endnu ikke er udviklet fuldt dækkende, implementerklare privacyløsninger til alle områder i samfundet. Kommercielle interesser i specielt infrastrukturen er også med til at blokere for en hensigtsmæssig udvikling, siger han.
Søren Duus Østergård foreslår, at man – på linie med lande som Finland og Sverige – opretter en ombudsmandsinstitution, der udelukkende beskæftiger sig med spørgsmål om databeskyttelse og privacy. En ombudsmand, man som privatperson kan klage til, hvis man fx føler sig gået for nær af et privat firmas markedsføring, eller hvis ens personlige data er blevet opsamlet, videregivet til andre og anvendt uretmæssigt.

Yderligere information

*__Stephan Engberg__, direktør i Open Business Innovation. Medlem af EU's Network of Excellence i relation til Privacy og Identity Management, medlem af Advisory Board for Privacy International. Deltog i
stephan.engberg@obivision.com,
www.obivision.com
*__Søren Duus Østergård__, Senior e-government advisor for IBM i Europa, Mellemøsten og Afrika. Medlem af Teknologirådets bestyrelse og arbejdsgruppe om IT-infrastrukturens sårbarhed.
sdo@dk.ibm.com.
*__Marit Hansen__, leder af afdelingen for Privacy Enhancing Technologies (PET's) på det uafhængige center for privacy beskyttelse i Slesvig-Holsten, ICPP. Deltager i en række EU-projekter, bl.a. PRIME (Privacy and Identity Management for Europe). Deltog i EU-workshop i juli 2003 om PET's.
marit.hansen@datenschutzcentrum.de
* Konklusioner og anbefalinger fra EU-workshop i juli 2003 om PET's, hvor både Stephan Engberg og Marit Hansen deltog:
http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/pet/200304-pet-outcome_en.pdf
* Arbejdsgruppen vedr. borgernes IT-rettigheder under Ministeriet for Videnskab, Teknologi og Udvikling, har givet en række anbefalinger, bl.a. om at undersøge om PET's kan være en tekniske løsninger til at øge borgernes tryghed på internet.
http://www.videnskabsministeriet.dk/fsk/div/itsoejlen/rettigheder_pdf.pdf
* Privacy International og Electronic Privacy Information Centre, to organisationer, der beskæftiger sig med borgernes rettigheder og interesser ang. privacy, står bag rapporten "Privacy and Human Rights – a survey of privacy laws and developments", med en oversigt over bl.a. alle EU-landes databeskyttelses/privacy love -
http://www.privacyinternational.org/survey/phr2003/

Fra rådet til tinget udgives af Teknologirådets sekretariat.
Dette nummer er skrevet af freelancejournalist Jakob Vedelsby og redaktør Ida Leisner

De sidste fem numre Fra rådet til tinget er:
185: Mens vi venter på ulykken
184: Pris på miljøet
183: Dårlig sikkerhed til hjemme-pc'en
182: EPJ også patientens værktøj
181: Effektiv overvågning af havmiljøet

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyhedsbreve findes på:
www.tekno.dk/rtt.htm