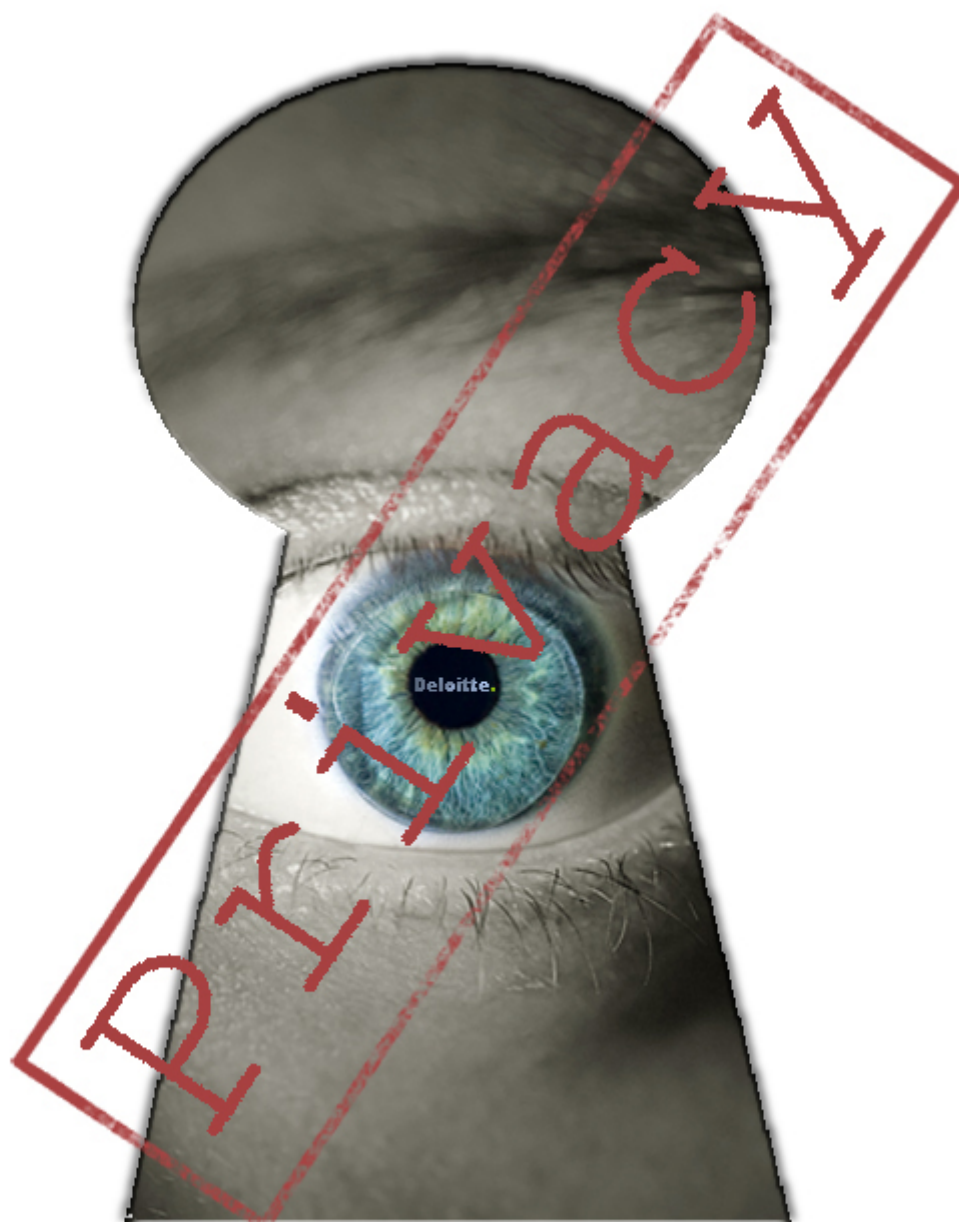


Nordisk Ministerråd
Store Strandstræde 18
DK-1255 København K
Telefon: 33 96 02 00
Fax: 33 96 02 02
nmr@norden.org

Deloitte
Statsautoriseret Revisionsaktieselskab
CVR-nr.: 24 21 37 14
H. C. Andersens Boulevard 2
1780 København V
Telefon 33 76 33 33
Telefax 33 76 39 93
www.deloitte.dk

Delrapport 2

-Kortlægning af potentielt privatlivsfremmende og -truende teknologier



'The right to be left alone'

1890 - Samuel D. Warren og Louis D. Brandeis

24. oktober 2005

Indholdsfortegnelse

	<u>Side</u>
Indledning	1
Omfang	2
Konklusion	2
Styringsmidler	3
Udvikling	4
Kultur	4
Teknologi	5
Teknologioversigt	6

Indledning

Delopgave 2 er en kortlægning af de teknologier, som potentielt kan medvirke til at undgå eller begrænse inddatering, opbevaring og udveksling af persondata.

Der findes ikke en komplet liste eller definition over privatlivsfremmende og –truende teknologier, også betegnet Privacy Enhancing Technologies (PET). En af årsagerne hertil er, at en sådan registrering hurtigt vil være forældet, da udviklingen inden for PET går meget stærkt.

Vi har som udgangspunkt studeret Gartners analyse kaldet "Hype Cycle for Emerging Technologies, 2005". Herudover har vi taget udgangspunkt i de mest gængse teknologier, som er integreret i samfundet i dag, og som er relevante i relation til borgernes privacy.

Omfang

Opgavens formål er at give et overblik over relevante teknologier i relation til it-privacy for borgerne i samfundet. Der er på baggrund af en dialog med NM og omfattende research på området udvalgt en række tidssvarende teknologier, som er implementeret i vid udstrækning, og som har eller vil få indflydelse på borgernes it-privacy.

Opgavens formål har ikke været at definere en grundlæggende og fuldstændig gruppering af anvendte teknologier, men at identificere og fokusere på praktisk anvendte teknologier, som er implementeret i samfundet i dag, eller som forventes implementeret i nærmeste fremtid.

Konklusion

Ud fra de udvalgte teknologier, vi har valgt at inkludere i denne rapport, har vi set på de dilemmaer, som de nordiske lande står med i relation til, at lovgivningen er i kontakt med den teknologiske udvikling.

Styringsmidler

Dilemmaer omkring styringsmidler

- ***Er det risikoen værd at satse borgernes mest personlige oplysninger for at effektivisere samfundet ved at koble centrale personregistre til Internettet, som man ikke har kontrol over eller midler til at styre?***
Der er mange gode grunde til at samle informationer i centrale databaser og gøre dem tilgængelige over internettet. Det letter administrationen og øger serviceniveauet. Hvis først privacy-relaterede informationer bliver frigivet på internettet ved en fejl eller i forbindelse med et hacker-angreb, så kan man ikke hive informationerne tilbage eller slette dem fra internettet igen, eftersom de efter kort tid vil ligge gemt i søgemaskinernes databaser og derved spredt ud over mange forskellige lande med forskellige lovgivninger. CPR-registre i Norden er så integreret i så mange systemer, at det vil være utroligt svært at ændre borgernes personnumre i tilfælde af, at de bliver publiceret på internettet.
- ***Hvis man fokuserer på lovgivning omkring konkrete teknologier, vil lovgivningen så kunne følge med den teknologiske udvikling?*** Der er mange nye teknologier, som giver mulighed for at registrere borgernes gøren og færden. RFID-chips i forbrugervarer bliver formentlig den næste store problemstilling, som de nordiske lande skal tage stilling til. Man kan vælge at lovgive omkring centrale teknologier, fordi visse centrale teknologier kan have meget stor indflydelse på borgernes privacy. Indtil videre har man primært fokuseret på oplysningerne frem for teknologierne i lovgivningen. Med RFID og mobiltelefoner, som indirekte giver mange informationer om borgerne, der dog ikke direkte betegnes som personfølsomme, er lovgivningen måske kommet til kort.
- ***Hvis man ønsker at lovgive i forhold til teknologier, kræver det, at man på en eller anden måde får dem grupperet eller kategoriseret evt. efter funktionalitet eller anvendelsesmulighed. Det er ikke klart, hvorledes det skal gøres.*** Det er ikke umiddelbart muligt at gruppere teknologierne i henholdsvis PIP og PEP teknologier, eftersom næsten alle teknologier har begge egenskaber. Det gør det komplekst at lovgive i forhold til PIP og PEP egenskaber for de forskellige teknologier.

Udvikling

Dilemmaer omkring udvikling

- *Er man villig til at effektivisere og indføre de nødvendige teknologier uden at have overblik over det informationspotential, der opbygges på internettet, og de privacy problemstillinger, der er relateret hertil?* Brugen af søgemaskiner er formentlig den mest effektive måde at finde specifikke informationer på Internettet. Søgmaskinerne er efterhånden så effektive, at de kan finde stort set alle dokumenter, der er publiceret på internettet inden for millisekunder. Indførslen af nye teknologier i samfundet betyder ofte, at flere informationer, herunder privacy-relaterede informationer, flyder frit og i visse tilfælde ender på internettet. Et bevis for dette er konceptet "Google hacking", hvor man simpelthen har opstillet nogle effektive søgekriterier, som for eksempel er rettet mod at finde kontooplysninger for Visa eller Mastercard, som fejlagtigt er blevet publiceret på internettet.

Kultur

Dilemmaer omkring kultur

- *Er de nordiske lande villige til at gå på kompromis med borgernes privacy for at effektivisere samfundet ved at tillade, at private og offentlige institutioner ukontrolleret opbygger privacy-relaterede databaser, fordi det er nemt med de nye teknologiske opfindelser?* Den store udvikling af it-systemer i det offentlige og i det private har medført, at borgernes privacy-relaterede informationer bliver registreret i databaser mange forskellige steder. I Danmark eksempelvis bliver CPR-nummer efterhånden benyttet af alle private institutioner og firmaer til at registrere borgerne. Det gør det nemt at sammenkoble bankinformationer, forsikringspolice og andre privacy-relaterede informationer. Få årtier tilbage var det helt utænkeligt at udlevere sit CPR nummer til en privat institution.

Teknologi

Dilemmaer omkring teknologi

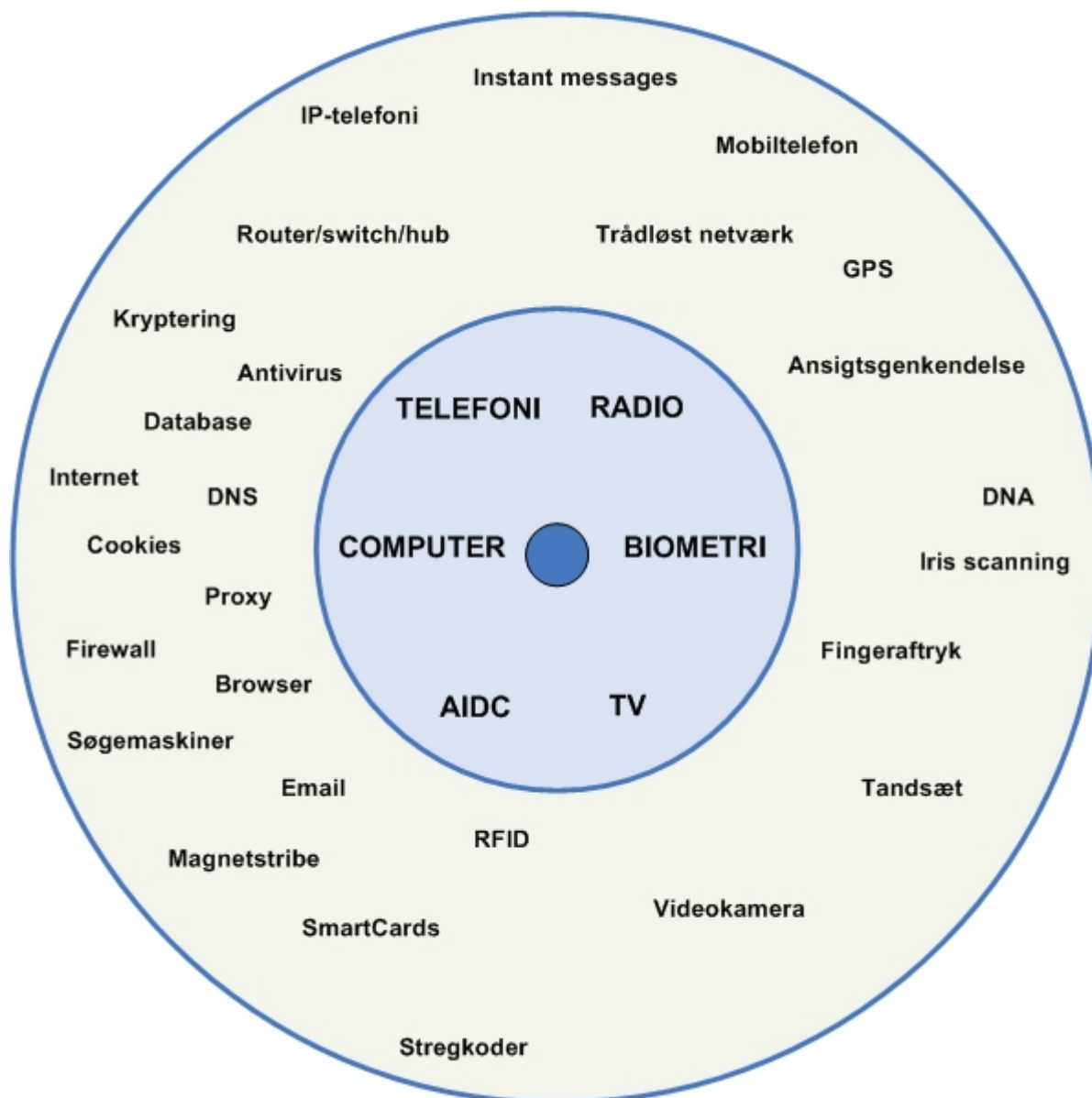
- ***Er prisen for høj i relation til privacy, og har staten ressourcer nok til at uddanne befolkningen til at være bevidste omkring konsekvenserne ved de nye teknologier?*** De mange nye teknologier, der bliver benyttet i samfundet i dag, er med til at højne serviceniveauet og effektiviserer dagligdagen for de nordiske landes borgere. De statslige institutioner arbejder mod papirløs sagsbehandling, og der vil formentlig være RFID chips i de fleste forbrugervarer inden for få år. Brugen af avancerede teknologier i samfundet er med til, at Norden er opdateret og førende inden for it-udvikling.
- ***Er det hensigtsmæssigt, at sådanne teknologier er tilladte og integrerede i forbrugerapplikationer for at fremme borgernes privacy, mod potentielt at kompromittere rigets sikkerhed?*** De moderne krypteringsteknologier giver muligheder for, at enhver kan kryptere data så kraftigt, at det ikke er praktisk muligt at afkode det igen uden den rigtige nøgle.

Teknologioversigt

Teknologioversigten lister udvalgte teknologier, som har været relevante i relation til privacy igennem de seneste årtier. De fleste teknologier, som er relevante i relation til privacy, er relateret til computerudviklingen på et eller andet plan. Computerne har tilført teknologiudviklingen følgende egenskaber, som er relevante i relation til privacy:

- **Lagerplads** – Moderne harddiske og databaseteknologi yder næsten ubegrænset lagerplads for lagring og opbevaring af persondata.
- **Analyse** – Med computerne er det muligt at søge på tværs af informationer globalt. Derudover er datamining blevet muligt på et helt nyt plan.
- **Størrelse** – Den nyeste udvikling af microchips har gjort computerne så små og billige, at mennesker i dagligdagen er tilkoblet langt flere PET- og PIT-teknologier.
- **Pris** – Computerkraft og lagerplads er blevet tilgængelig for en langt større brugergruppe, selv private brugere har i dag i vid udstrækning ressourcer til at opbygge omfattende databaser og lave komplekse analyser.

Figur 1 - Teknologioversigt, viser et diagram over de valgte teknologier. Diagrammet fungerer som indeks, da de angivne teknologier i yderste kreds er medtaget med forklaring i den følgende tabel. Den inderste cirkel i figuren repræsenterer sammenkoblede teknologier, også kaldet konvergens produkter, såsom 3G mobiler, der indeholder både videokamera, kamera og mobiltelefon. Den yderste ring angiver konkrete teknologier, som til dels anvendes i samfundet i dag, og som er relevante i relation til personfølsomme oplysninger.



Figur 1 - Teknologioversigt

I tabellen herunder beskrives de forskellige teknologier svarende til Figur 1, og centrale "privacy enhancing" og "privacy invasive" egenskaber er angivet.

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
Database Databaser fortolkes i en bred kontekst som alle elektroniske data-	Registrering i databaser gør det lettere at finde specifikke informationer i store datamængder.	Personinformationer kan gemmes centralt, således at adgangen kan kontrolleres og begrænses mest mu-	Databaser kan bruges til at indsamle store mængder informationer hurtigt og automatiseret. Desuden er der

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
lagre. Konkrete eksempler på databaser, der relaterer til personfølsomme oplysninger inkluderer fx Elektroniske Patient Journal (EPJ). Bankernes database om økonomiske forhold og personlige informationer samt ePosthuset, der digitalt opbevarer folks post.	Dertil kommer, at registrering i databaser er billigt, hurtigt og i høj grad kan automatiseres. Endvidere betyder billig lagerplads, at der kan gemmes flere informationer i længere tid.	ligt.	<p>gode muligheder for at genfinde data hurtigt og lave komplekse dataudtræk over mange parametre.</p> <p>Den store udbredelse af databaser betyder dog, at informationer om borgerne bliver spredt ud, og det betyder, at borgerne såvel som staten mister kontrollen med, hvem der har adgang til personfølsomme oplysninger.</p> <p>Virkemidler: Streng sikkerhedskontrol ved adgangen til databaser og specifik brugertilladelse ved udlevering af data fra databaser, hvor meget personfølsom data er opbevaret.</p>
<p>Internet</p> <p>Internet omfatter alle de komponenter, som er nødvendige for at kommunikere globalt. Internetinfrastrukturen bygger på en række grundelementer, herunder routere og swit-</p>	<p>Internettet gør det let at eksponere data og databaser globalt og giver næsten ubegrænsede muligheder for søgning og "data-mining" globalt.</p> <p>Den åbne struktur</p>	<p>Internettet gør det muligt at besidde en virtuel identitet, som ikke kan kædes til ens fysiske person.</p>	<p>Internettet letter adgangen til informationer globalt i en udstrækning, der er ikke set førhen. Internetkommunikation er efterhånden en så integreret del af samfundet, at det er på højde med telefonnet-</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
<p>che. Derudover er der en række aktive komponenter, som segmenter og sikrer Internettet, herunder firewalls og proxy-servere.</p>	<p>af Internettet og den begrænsede lovgivning giver uanede muligheder for trafiklogging og analyse af kommunikation.</p>		<p>tet.</p> <p>Internettets eksponering af oplysninger giver adgang til uanede mængder data og gør specifikke søgninger muligt, hvor data kan sammenholdes og analyseres. Kaldes også datamining.</p> <p>Internettet er endvidere forbundet til et stort antal databaser med personfølsom data, hvortil der potentielt kan opnås uautoriseret adgang med rette værktøjer og/eller viden.</p> <p>Virkemidler: Anonymiseringsværktøjer, der sikrer sløring af IP- og MAC-adresse ved aktivitet på nettet.</p>
<p>Proxy</p> <p>Proxy betyder oprindeligt stedfortræder eller en, som har lov til at handle på vegne af en anden. En proxy-server er netop en</p>	<p>Det er ikke altid muligt at fastslå, om man passerer en proxy-server. Er det tilfældet, er det ikke klart, hvem der har adgang til de informationer, en proxy-</p>	<p>Proxy-servere kan benyttes til at anonymisere internetbrugere fuldstændigt. Desuden kan proxy-serverne filtrere trafik, således at brugerne undgår visse typer af trafik.</p>	<p>En proxy-server bruges til at beskytte brugerne mod trusler fra internettet. Den filtrerer applikationsdata, således at ondsindet data ikke når frem til slutbrugerne.</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
server, som står imellem afsender og modtager. Kun proxy-serveren har kontakt med de to kommunikerende parter. Denne konstellation betyder, at proxy-serveren kan gøre således, at de to kommunikerende parter ikke får nogle oplysninger om hinanden.	server opsamler, eller de statistikker, den typisk opbygger.	Kan beskytte mod trojanske heste og orme, som ofte benyttes til identitetstyveri.	Proxy-servere er knudepunkter, der kan benyttes til at overvåge alt trafik og dermed misbruges til at overvåge enkelte brugere, der benytter en proxy-server. Virkemidler: Streng adgangskontrol til informationer, som proxy-serveren samler.
Firewall Firewalls benyttes til at filtrere trafik, således at kun den trafik, man ønsker, slipper igennem.	Ofte vil en firewall være et krydsfelt, som alt datatrafik passerer, derfor benyttes firewalls ofte som kilde til central logging og registrering af datatrafik. Det er ikke altid muligt at vide, om man passerer en firewall, og det er slet ikke muligt at vide, hvad der bliver logget, og hvorledes det bliver brugt efterfølgende.	En korrekt konfigureret firewall kan beskytte brugeren for irrelevant information såvel som destruktive programmer, herunder trojanske heste og orme, som ofte benyttes til identitetstyveri.	En firewall beskytter brugeren, som er koblet på netværket, mod uønsket trafik. Herunder virus og orme. En firewall er et trafikknudepunkt og kan misbruges til at overvåge enkelte brugere. Virkemidler: Streng adgangskontrol til informationer, som firewallen samler.
Router/switch/hub Er de aktive komponenter, som internettet er bygget op omkring,	Alle de aktive komponenter, som internettet er bygget op omkring kan i princippet benyttes	Nogle routere og switcher har primitive firewall-egenskaber og kan derfor beskytte brugerne mod udefra-	De kan segmentere og opdele netværk, dels for at forhindre flaskehalse i datatrafikken, dels for at lave

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
og som håndterer alle de datapakker, der benyttes til at kommunikere verden over.	til at logge og registrere brugernes trafikmønstre og endda overvåge deres kommunikation.	kommende.	adgangsbegrænsninger til dele af et netværk. Routere, switche og hubs er infrastrukturkomponenter, der fungerer som knudepunkter for datatrafik, derfor kan de misbruges til at overvåge og monitorere enkelte brugere. <hr/> Virkemidler: Streng adgangskontrol til informationer, som komponenterne samler.
Kryptering Digital signatur og SSL-kryptering af websider er blandt de mest udbredte praktiske anvendelser af kryptering i samfundet.	Staten i Danmark og alle offentlige institutioner bygger på kryptering med digital signatur. Det er dog ikke klart, hvem der har en kopi af de private nøgler, der bliver udstedt, hvor og hvor sikkert de opbevares, og hvor mange kopier der eksisterer.	Information kan beskyttes, så kun afsender og modtager kan afkode informationen. Udbredelsen af computere og krypteringssgoritmer har gjort stærk kryptering til hver mands eje.	Med datakryptering, herunder digital signatur og SSL-webkryptering kan data sikres på et højt niveau, hvorved der kan undgås uautoriseret adgang til personfølsomme data. Ved brug af stærk kryptering kan netværkstrafik ikke overvåges eller dekodes. Ikke engang staten har ressourcer til at bryde stærk kryptering. <hr/> Virkemidler:

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
			Centralisering af administration af digital signatur og SSL-certifikater øger sikkerheden i teknologierne.
<p>Browser</p> <p>En browser er et program, der benyttes til at fortolke HTML-koder. HTML-koder kan indeholde information om teksformatering, billedopstilling og links. Generelt betegnes data bestående af HTML som web-sider.</p>	<p>Et stadigt stigende antal websider benytter pop-ups til at fange brugerens opmærksomhed, hvorved brugeren ikke har kontrol over, hvilke vinduer der åbnes på computeren. Der lagres cookies lokalt på brugerens maskine, som efterlader et spor over, hvilke websites, en bruger har besøgt.</p>	<p>Kompleks information bestående af tekst, lyd og billede kan tilgås anonymt over internettet.</p>	<p>Browseren gør det muligt at tilgå informationer anonymt over internettet.</p> <p>Den indeholder typisk faciliteter, herunder cookies og cache, der lagrer oplysninger om brugerens trafik/historik på internettet.</p> <hr/> <p>Virkemidler:</p> <p>Brug af SSL-kryptering, som giver sikker adgang til web-sider.</p> <p>Brug af anti pop-up og adware værktøjer samt firewall, der mindsker adgangen til borgerens pc.</p>
<p>Email</p> <p>Begrebet dækker over det software, som benyttes til at sende og modtage emails. Dels er der email-</p>	<p>Det er ikke klart, hvor mange kopier af ens beskeder, der bliver lagret.</p> <p>Det er ikke klart, hvor ens beskeder</p>	<p>Man kan sende beskeder anonymt og hurtigt.</p> <p>Det er muligt at tilføje kryptering til emails, således at de ikke kan</p>	<p>Email er en løsning, så man globalt og uden begrænsninger kan sende beskeder til hinanden. En email er typisk fremme på destinationen på få se-</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
klienterne, dels er der mail-serverne, som står for at analysere og transportere emails.	<p>bliver lagret, og hvor godt de er beskyttet.</p> <p>Det er ikke klart, hvad ens beskeder bliver brugt til, og hvor lang tid de bliver lagret.</p> <p>Da man kan sende beskeder anonymt og gratis, er det muligt at sende reklamer ud til hvem som helst, uden at de har bedt om det – det kaldes populært "spam".</p> <p>Det kan være svært og endda umuligt at kontrollere, hvilke og hvor mange emails man vil modtage. Derfor benyttes email ofte til udsendelse af "spam" og ondsindet kode i form af vira.</p>	læses, medmindre man kender krypteringsnøglen.	<p>kunder.</p> <p>Det ikke klart, hvilken rute en email har rejst over internettet pga. den måde protokollen er designet på, og derfor er det ikke muligt at finde ud af, hvor mange kopier der er lagret rundt omkring, og hvem der har adgang til at læse disse kopier.</p> <hr/> <p>Virkemidler: Brug af digital signatur eller anden kryptering, der sikrer indholdet.</p>
<p>Instant messages</p> <p>Dækker over alle typer af "real time" chat applikationer, hvor beskeder popper op på</p>	<p>Der er samme problemstillinger som med e-mail.</p> <p>Ofte kan man detektere on-line/off-</p>	Man kan kommunikere anonymt og krypteret ligesom med e-mail, men det er interaktivt og "real time".	Chat-protokoller gør, at man kan kommunikere realtime over internettet globalt. Det er meget udbredt og hensigtsmæssigt i

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
<p>modtagerens skærm, så snart de er sendt. Det er i modsætning til email, hvor der kan gå mange sekunder, minutter eller timer, før den når frem.</p>	<p>line status, selv på folk man ikke kender.</p>		<p>mange henseender.</p> <p>Ofte vil chat-programmerne afsløre, om man er on-line. På grund af internettets opbygning, er det ikke klart, hvilken rute chat-trafik rejser over internettet og derfor ikke klart, om nogen lytter med.</p> <hr/> <p>Virkemidler: Kryptering af trafik, der sendes via chat-programmer, sikrer, at oplysninger ikke slipper ud.</p>
<p>Søgemaskiner</p> <p>Søgemaskiner er i virkeligheden firmaer, som stiller meget store computerressourcer til rådighed for at kunne indekserer hele internettet og lave et interface, hvor man så kan søge i den omfattende database.</p>	<p>Man har ikke kontrol eller viden om, hvilke informationer der er gemt om ens egne aktiviteter på internettet. Det er heller ikke klart, hvorledes informationerne bliver brugt, og hvem der har adgang til dem.</p>	<p>Man kan søge anonymt i informationer globalt.</p>	<p>Det er nødvendigt med grundig indeksering og en stor databaseinfrastruktur for at kunne søge informationer globalt på en overskuelig måde. Der bruges store ressourcer af søgemaskinefirmaerne på at høste så mange informationer som muligt fra internettet for at kunne give de mest præcise resultater.</p> <p>Søgemaskiner giver mulighed for anonym</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
			<p>søgning af oplysninger i forhold til f.eks. udlån på biblioteket, hvor udlånsoplysninger registreres.</p> <p>De effektive søgemaskiner betyder, at der ligger meget personrelaterede data i store kommercielle databaser. Søgemaskinerne gør det muligt at lave avanceret datamining for alle.</p> <hr/> <p>Virkemidler: Sikre søgemaskiner, der ikke giver tilladelse til at søge på specifikke personer eller bestemte søgeord medmindre tilladelse er givet af vedkommende.</p>
<p>DNS</p> <p>Domain Name Server (DNS) er en række store databaser, der indeholder IP-numre og web-adresser, således at internetbrugere kan benytte de mere brugervenlige internetadresser i modsætning til IP-numre, som of-</p>	<p>DNS-infrastrukturen kan benyttes til at indsamle detaljeret information om virksomheders, private og offentlige institutioners internetperimeter.</p>	<p>Web-adresser kan registreres anonymt i DNS-servere, så man kan eksponere sine informationer under en let tilgængelig adresse, uden at ejeren kan identificeres.</p>	<p>DNS giver adgang til en global infrastruktur, der kan benyttes til at sammenkoble IP-numre og internetadresser. Det er en vigtig bestanddel i, at internettet fungerer i praksis.</p> <p>DNS-infrastrukturen kan give nyttige in-</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
test er sværere at huske for mennesker.			<p>formationer, som kan bruges i forbindelse med at opnå uautoriseret adgang til en Internetperimeter.</p> <hr/> <p>Virkemidler: Lukning af søgema- skiner såsom WHOIS eller kun adgang til informationer igennem tilladelse.</p> <p>Lukning af muligheder for at gennemføre ping, tracert, DNS lookup mv.</p>
<p>Antivirus</p> <p>Ligesom der findes computervira, findes der antivirussoftware, der sørger for konstant at scanne efter og eventuelt fjerne computervirus.</p>	<p>Antivirusprogrammer overvåger al data på en computer. Typisk opdaterer de sig selv over internettet. Nogle antivirusprogrammer melder tilbage til producenten om, hvilke vira der er registreret og afgiver derfor informationer om, hvilke vira man har været smittet med.</p>	<p>Blokerer en række uønskede programmer og forhindrer derved, at hackere, orme eller andre får adgang til computere og data.</p>	<p>Antivirus forsøger at stoppe computervira, inden de eksekveres. Det beskytter brugerne mod ondsindet programmel.</p> <p>Antivirusprogrammerne kræver opdateringer med høj frekvens, og derfor kontakter de ofte automatisk centrale opdateringsservere. I den forbindelse lagres informationer om status på den enkelte computer.</p> <hr/> <p>Virkemidler: Godkendelsen til au-</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
			<p>tomatisk download af opdatering skal gives af brugeren.</p> <p>Oplysningspligt vedrørende information, som antivirusprogrammet indsamler.</p>
<p>Mobiltelefon</p> <p>Mobiltelefoner er efterhånden en form for hybridteknologi, der ud over telefonfunktionen indeholder kalender, kontaktpersoner og andre personrelaterede informationer.</p>	<p>Position af aktiv mobiltelefon kan bestemmes inden for få 100 meter, blot den er tændt, idet telefonen konstant kommunikerer med omkringliggende mobilmaster.</p> <p>Mobil kommunikation kan logges og relateres til en bestemt abonnent.</p>	<p>Man kan koble anonymt på telefonnettet, ligesom når man benytter en telefonboks. Yderligere kan man frit skifte position, mens man kommunikerer.</p> <p>Brug af taletidskort gør ens kommunikation anonym.</p>	<p>Mobiltelefoner giver mulighed for frit at bevæge sig rundt, mens man benytter telefonnettet.</p> <p>Mobiltelefoner kommunikerer ved at koble trådløst op til stationære mobilmaster, som dirigerer trafikken ind på telefonnettet. Herved er det muligt at triangulere, hvor den aktive mobiltelefon har befundet sig på et givent tidspunkt.</p> <p>Virkemidler:</p> <p>Brug af anonymt taletidskort eller mulighed for at fjerne navn- og adresseoplysninger om personen bag nummeret.</p>
<p>Trådløst netværk</p> <p>Trådløst netværk dæk-</p>	<p>Det er langt sværere at lave fysisk sikkerhed omkring et</p>	<p>Man kan koble anonymt op på internettet vha. offentligt tilgæn-</p>	<p>Trådløse netværk gør det nemt og mobilt at kommunikere data.</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
ker over de trådløse teknologier, der benyttes i forbindelse med computerdatanetværk, i modsætning til telefonnetværk. Trådløst netværk dækker trådløse "access points" og "hot spots" og radio-kædeteknologi, der benyttes i forbindelse med trådløs backbone-teknologi.	trådløst datanetværk og dermed begrænse udefrakommende, der ønsker at kompromittere informationer.	gelige hotspots.	<p>Ved trådløs datakommunikation er det ikke umiddelbart muligt at bestemme, hvilke enheder man fysisk har kontakt med. Ligeledes er det ikke muligt at bestemme udstrækningen af signalet, og derved hvem der lytter med.</p> <hr/> <p>Virkemidler: Stærk kryptering af trådløs datakommunikation sikrer imod eksponering af personlige oplysninger.</p>
<p>GPS</p> <p>GPS (Global Positioning System). GPS-udstyr kan ved at triangulere mellem flere satellitter bestemme den nøjagtige position på jordkloden ned til få meters afstand. GPS virker kun udendørs.</p>	GPS-enheder er efterhånden relativt små og kan derfor monteres på mange forskellige ting og benyttes til at monitorere positionen af et objekt ned til få meters afstand.	Ingen.	<p>GPS er det moderne kompas, der giver mulighed for, at brugerne kan bestemme deres nøjagtige position på jordkloden ned til få meters præcision.</p> <p>GPS kan være indbygget i alt fra biler til både og mobiltelefoner og kan bruges til at overvåge den nøjagtige position af en genstand.</p> <hr/> <p>Virkemidler: Sikker opbevaring af GPS-data.</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
<p>Videokamera</p> <p>Den digitale udvikling har gjort videokameraer billige, automatiserede og driftsikre.</p> <p>Selv de nyeste mobiltelefoner har mulighed for at optage, lagre og afspille video.</p> <p>Ligesom man via sin computer og internettet kan vise video med et web-kamera.</p>	<p>Kameraovervågning af det offentlige rum bliver mere og mere udbredt i lande i og omkring Europa.</p> <p>Kameraerne kan produceres så små, at de i dag er integreret i mobiltelefoner, hvilket vil sige, at privacy i det offentlige rum både er truet af statens øgede overvågning og private optagelser, der publiceres og offentliggøres ukontrolleret.</p> <p>Når video lagres digitalt, er der øgede muligheder for billedbehandling og analyse af optagelser, hvilket kan benyttes til at kæde hændelser sammen, som før ville have været praktisk umuligt.</p>	<p>Man kan præsentere sig selv på en videooptagelse og behøver ikke nødvendigvis at være i fysisk kontakt med de mennesker, som ser en.</p>	<p>Videoovervågning bliver mere og mere udbredt i det offentlige rum, fordi det giver en vis tryghed for borgerne og kan være med til at forebygge kriminalitet.</p> <p>Borgerne bliver overvåget, uden at de er bevidste herom. Når man går ind i en bank eller et tog, er der den dag i dag stor sandsynlighed for, at man bliver filmet, og flere og flere steder bredes videoovervågningen ud i det offentlige rum.</p> <hr/> <p>Virkemidler:</p> <p>Lovpligtig oplysning om overvågning på offentlige steder informerer borgerne om, at videoovervågning bliver foretaget.</p> <p>Godkendelse til overvågning på offentlige steder skal være på plads.</p>
IP-telefoni	Når telefonsamtaler	Internettet kan bruges	Med IP telefoni er det

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
<p>Telefonien er langsomt ved at bevæge sig over på det globale internet. Dels fordi nettet er billigere at benytte, dels fordi det åbner helt nye muligheder for at kombinere telefoni og computerteknologi.</p>	<p>bevæger sig over internettet, er det ikke længere klart, hvem der styrer det aktive udstyr, som en telefonsamtale passerer. Førhen var det ofte statskontrollerede kabelnet og teleudbydere, der stod for telekommunikationen. I dag kan det være hvem som helst, der er koblet på internettet. Samtidig kan aflytning ske alene ved hjælp af software og kræver ikke nødvendigvis fysisk adgang til hardware, så som telefonkrydsfelter eller telefonkabler.</p>	<p>til fuldstændig anonym telefonkommunikation.</p> <p>Brugeren kan tilføje kryptering og på den måde gøre sine telefonsamtaler sikre for omverdenen.</p>	<p>blevet muligt at ringe med lokaltakst til alle telefoner i verden. Det er ofte gratis at ringe fra en IP telefon til en anden, ligegyldig hvor på jorden den befinder sig.</p> <p>Det er ikke længere gennemskeligt, hvilke krydsfelter og omstillingscentraler teletrafik passerer, og hvad der monitoreres.</p> <hr/> <p>Virkemidler: Kryptering af trafik, der sendes over internet.</p>
<p>DNA</p> <p>Alle menneskets celler indeholder DNA, som indeholder komplette koder til at opbygge et helt menneske. Ved at lave en DNA-test kigger man på dele af DNA, som typisk varierer fra menneske til menneske.</p>	<p>Et centralt DNA-register, der er knyttet til personfølsomme oplysninger, vil betyde, at hvert menneske bliver unikt identificeret og ikke har mulighed for at ændre denne identitet.</p> <p>Dette er sådan set generelt for de fle-</p>	<p>Man behøver ikke at opgive traditionelle, personfølsomme oplysninger, som pasnummer, navn, adresse og personnummer. Det kræver store ressourcer at kæde DNA til personfølsomme oplysninger.</p>	<p>DNA betragtes som et unikt aftryk af et menneske. Der er ikke mulighed for at ændre dette aftryk med dagens teknologier. Derfor er det oplagt at bruge som identifikation af et menneske.</p> <p>DNA indeholder informationer om men-</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
	ste biometriske aftryk.		neskers opbygning, og derfor kan det bruges til at udarbejde en meget detaljeret profil af et menneske. <hr/> Virkemidler: Sikker opbevaring af oplysninger vedr. DNA-data ved f.eks. streng adgangskontrol til databaser hvor disse oplysninger opbevares.
Iris scanning Iris er selve formationerne i øjet. Disse formationer er genereret ud fra vores DNA.	Giver et relativt unikt billede af øjets Iris og dermed en relativ unik biometrisk identifikator af et menneske.	Man behøver ikke at opgive traditionelle personfølsomme oplysninger, som pasnummer, navn, adresse og personnummer.	Øjets iris betragtes som et unikt aftryk for et menneske. Samtidig er det nemmere at aflæse end for eksempel DNA. Ved at opbevare informationer om øjets iris har man en unik fysisk identifikator af et menneske. <hr/> Virkemidler: Sikker opbevaring af oplysninger vedr. iris-data ved f.eks. streng adgangskontrol til databaser hvor disse oplysninger opbevares.
Fingeraftryk Det er omkring 100 år	Giver et relativt unikt biometrisk aftryk af et menne-	Man behøver ikke at opgive traditionelle personfølsomme op-	Fingeraftryk benyttes i praksis i dag og gør det nemmere at identi-

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
<p>siden, man begyndte at affotografere fingeraftryk som et biologisk aftryk af et menneske. Med dagens teknologier kan man efterligne og ændre et menneskes fingeraftryk. Derfor kan det ikke længere betragtes som det stærkeste biometriske aftryk.</p>	<p>ske. Fingeraftryk er dog en gammel teknologi, og i dag er det både muligt at kopiere og ændre et fingeraftryk.</p>	<p>lysninger, som pasnummer, navn, adresse og personnummer, hvis der benyttes fingeraftryk som identifikation.</p>	<p>ficere sig selv hurtigt og bekvemt uden at skulle have magnetkort, pas eller anden identifikation med.</p> <p>I dag er det muligt at kopiere og efterligne fingeraftryk, og derfor betragtes det ikke længere som en rigtig sikker identifikator.</p> <hr/> <p>Virkemidler: Sikker opbevaring af oplysninger vedr. fingeraftryks-data ved f.eks. streng adgangskontrol til databaser hvor disse oplysninger opbevares.</p>
<p>Ansigtsgenkendelse</p> <p>Ligesom de andre biometriske aftryk bygger ansigtsgenkendelse på en række fysiske træk i vores ansigtsstruktur, der kan benyttes som biometrisk aftryk for et menneske.</p>	<p>Dimensionerne af et ansigt kan i høj grad sandsynliggøre genkendelse af en person.</p>	<p>Man behøver ikke at opgave traditionelle personfølsomme oplysninger, som pasnummer, navn, adresse og personnummer.</p>	<p>Ansigtsgenkendelse er en anden biometrisk identifikator, der kan bruges til nemt og hurtigt at identificere sig.</p> <p>Ansigtsgenkendelse benyttes allerede i lufthavne og andre steder. Det er ikke klart, hvem der har adgang til de data, der lagres.</p> <hr/> <p>Virkemidler: Sikker opbevaring af</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
			oplysninger vedr. ansigtsgenkendelses-data ved f.eks. streng adgangskontrol til databaser hvor disse oplysninger opbevares.
<p>Tandsæt</p> <p>Tandsæt er et af de mest anvendte biometriske aftryk, især i forbindelse med brandulykker, hvor tænderne ofte er det eneste, der kan klare de høje temperaturer og stadigvæk giver et relativt unikt biometrisk aftryk af et menneske.</p>	<p>Tandlæger opbevarer ofte detaljerede journaler om folks tandsæt. Ligeledes vil de ofte have registreret folk ved personnummer. Det er ikke klart, hvor langt den digitale udvikling er nået inden for tandlægebranchen, og hvordan disse informationer er beskyttet.</p>	Ingen.	<p>Tænderne er ofte noget af det sidste, som går til i forbindelse med brand eller eksplosioner og er derfor et meget udbredt biometrisk aftryk til identifikation af mennesker.</p> <p>Tandlæger besidder ofte databaser over menneskers unikke tandsæt.</p> <hr/> <p>Virkemidler: Sikker opbevaring af oplysninger vedr. tandsæts-data ved f.eks. streng adgangskontrol til databaser hvor disse oplysninger opbevares.</p>
<p>RFID</p> <p>Radio Frequency ID er blevet spået til at blive den største trussel mod privacy i det 21. år-</p>	<p>RFID er produceret til en størrelse på 0,4 mm. Derfor kan de fleste fysiske objekter i vores hverdag markeres</p>	<p>Automatisk maskine-til-maskine kommunikation (M2M) betyder, at det ikke kræver menneskelig overvågning at optælle eller</p>	<p>RFID giver mulighed for at aflæse informationer trådløst og automatisk. Dette kan lette og automatisere en masse arbejdsgange</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
<p>hundrede. RFID-chips er små radiochips, som kan afgive en unik kode, hvis man sender en forespørgsel ved hjælp af et radiosignal. RFID kan få energi fra det radiosignal, de modtager, og er derfor uafhængige af strømforsyning eller batterier. Det betyder, at de kan være meget små, og de kan holde meget længe. RFID-chippen kan i modsætning til magnetkort og stregkoder aflæses trådløst og uden "line-of-sight".</p>	<p>og registreres. Da kommunikationen er trådløs M2M-kommunikation, er det svært for en bruger at bestemme omfanget og typen af den kommunikation, der foregår.</p> <p>Aflæsning kræver blot, at der ikke er radioblokerende materialer mellem "Tag" og aflæser.</p>	<p>registrere fysiske enheder. Derfor bliver det ikke nødvendigt at have mennesker til at overvåge ens handler og transaktioner.</p>	<p>i vores samfund.</p> <p>Det er ikke nødvendigvis muligt at finde ud af hvor og hvornår, de RFID-tags, man er i kontakt med, bliver aflæst.</p> <hr/> <p>Virkemidler:</p> <p>Tydelig information på produkter, som indeholder RFID-chips, og mulighed for fjernelse eller deaktivering af denne.</p> <p>Oplysningspligt omkring aflæsning og registrering af RFID-chips.</p>
<p>Magnetstribe</p> <p>Traditionelle betalingskort, lånerkort og sygesikringskort er alle magnetstribe, hvor alle informationer er kodet ind i en magnetstribe, der kan aflæses automatisk.</p>	<p>Magnetstriber kan indeholde detaljerede informationer, som kan aflæses hurtigt af automatiserede systemer, hvilket gør det effektivt til at registrere informationer gentagne gange. De færreste forbrugere er klar over, præcis hvilke informationer de afgiver, når de benytter deres magnetkort til</p>	<p>Magnetstriber kan ikke aflæses med det blotte øje og kan derfor beskytte vores personlige oplysninger.</p>	<p>Hurtig og automatisk registrering af oplysninger i forbindelse med pengetransaktioner eller lægebesøg har gjort magnetstriber til hver mands eje.</p> <p>Brug af magnetkort registreres med tidspunkt og lokation. Derfor kan det bruges til at overvåge.</p> <hr/> <p>Virkemidler:</p> <p>Oplysningspligt omkring aflæsning og</p>

Teknologioversigt			
Anvendt teknologi	"Privacy Invasive" Potentialer	"Privacy Enhancing" Potentialer	Udfordringer
	forskellige formål. Kræver fysisk kontakt med aflæseren.		registrering af magnetstribekort-data.
Stregkoder Koder, der kan aflæses fra afstand ved hjælp af lysstråler. Stregkoder kræver "line-of-sight".	Gør det muligt hurtigt at registrere detaljerede oplysninger om fysiske objekter. Kræver "line-of-sight".	Kan ikke umiddelbart aflæses af mennesker. Stregkoder kan ikke aflæses direkte af mennesker.	Stregkoder giver mulighed for hurtig automatiseret og næsten fejlfri aflæsning af informationer. Stregkoder kræver "line-of-sight". <hr/> Virkemidler: Oplysningspligt omkring aflæsning og registrering af stregkode-data.
SmartCards SmartCards dækker over alle de nye typer kort, hvor informationerne er gemt i en chip i stedet for i den traditionelle magnetstriben.	Som forbruger er det ikke klart, hvad der er registreret på kortet, og det er heller ikke klart, hvad der bliver aflæst, når man benytter sit SmartCard.	Oplysningerne er skjult på en chip, som ikke kan aflæses umiddelbart af mennesker. Der kan være indbygget kryptering, så kun chipproducenten kan aflæse chippen.	Moderne alternativ til magnetstriben, som kan rumme flere informationer, og med mulighed for at sikre dem bedre. Brug af smartcards registreres med tidspunkt og lokation. <hr/> Virkemidler: Oplysningspligt omkring aflæsning og registrering af smartcard-data.