Dag Wiese Schartum og
Anne Gunn B. Bekken (red.)

YULEX 2011

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 978-82-7226-139-8
ISSN 0806-1912

Utgitt i samarbeid med Unipub
Trykk: AIT e-dit AS
Omslagsdesign Kitty Ensby

FORORD

Hvert år oppfordrer vi våre forskere til å gi bort en artikkel til jul. Vi pakker bidragene inn og sender dem som Yulex og julehilsen til SERIs mange samarbeidspartnere og kontakter. Som i tidligere har årets bok blitt en forundringspakke med et innhold vi håper du får glede av.

Når vi nå nærmer oss 2012 består kjernemiljøet ved Senter for rettsinformatikk av i alt 24 personer, blant dem seksten forskere. I tillegg er tolv forskere ved andre deler av Det juridiske fakultetet i Oslo og andre akademiske institusjoner knyttet til senteret.

Vi er glade over å kunne se tilbake på et år med forskningsaktiviteter og undervisning over bred front. I Yulex viser vi fram noe av mangfoldet i forskningen vår. Det kan derfor være på sin plass også å minne om at Senter for rettsinformatikk med Avdeling for forvaltningsinformatikk (AFIN) er ansvarlige for et bachelorprogram og to masterprogrammer innen vårt fagområde, med rundt regnet 200 eksamenskandidater per år. I tillegg kommer eksamener på flere enkeltemner.

Undervisningen på masternivå er langt på vei forskningsbasert, og målet er selvsagt at dyktige studenter selv får lyst og anledning til å forske og videreutvikle retts- og forvaltningsinformatikken. Det er derfor en glede å kunne konstatere at flere av våre forskere er rekruttert fra undervisningsprogrammene vi tilbyr. Noen av dem bidrar til dette årets utgave av Yulex.

God jul og godt nytt år!

PREFACE

Every year, we ask our researchers to contribute with an article as Christmas present. Articles they give are wrapped up by the Norwegian Research Center for Computers and Law (NRCCL) as Yulex, and sent to friends and partners of the Center. Like previous years, Yulex 2011 has turned out to be a surprising academic mix which we hope you will enjoy.

On the threshold of the year 2012, the NRCCL is housing 24 people and among them, at the heart of the Centre, sixteen researchers. In addition twelve members of the Centre with primary association to other parts of The Law Faculty of Oslo and institutions outside our university are affiliated with the NRCCL.

We are happy to look back on a year with broad and challenging research and educational activities. Yulex demonstrates some of the diversity of our research. Therefore, it may be appropriate to remind the reader that the NRCCL, with its Section for eGovernment Studies, offers three study programmes; one bachelor's programme and two master's programmes within our special field. Every year more than two hundred individual exams are submitted within our study programmes and other courses we offer.

Our lectures on master's level are to a large extent research based, and our aim is of course that competent students will have motivation and chance to develop their own research projects and contribute to our research field. Therefore, I am happy to note that several of our researchers have been recruited from our master´s programmes. Some of them are even contributing to this year's edition of Yulex.

Have a merry Christmas and a happy New Year!

CONTENTS

PERSONVERNANEKDOTER

Jon Bing

1 Prince Albert v Strange

Dommen *Prince Albert v Strange* (High Court of Chancery 1849) fremheves ofte som den første dommen som anerkjente personvern i engelsk rett.

Dronning Victoria og Prince Albert **Eos,** *Belgravia Gallery*

I 1848 fikk prins Albert en midlertidig beføyelse for å hindre en forlegger, William Strange, å utgi en katalog med beskrivelser av raderinger som han og dronning Victoria hadde skapt – blant disse var portretter av dem selv, prinsen av Wales, prinsessen og andre medlemmer av den kongelige familie. Det var scener fra barneværelset, og bilder av favoritthundene deres. Det var også reproduksjoner av gamle og sjeldne graveringer i dronningens eie. Flere av bildene var tegnet av dronningen etter levende modeller, og var senere overført til kobber av henne og prinsen. Opprinnelig ble raderingene reprodusert ved hjelp av en privat presse som de kongelige hadde anskaffet til dette bruket, og dronningen oppbevarte platene nedlåst. Enkelte av trykkene hang i dronningens egne værelser på Windsor.

Noen av raderingene ble sent til Middleton, en trykker i Windsor, for reproduksjon, slik at de kunne brukes som gaver til personlige venner. En av de ansatte hos trykkeren, Judge, laget noen kopier ekstra, og solgte disse til Strange, som ville vise dem offentlig i Egyptian Hall eller et annet galleri med like høyt renommé. Judge hadde skrevet en katalog for denne utstillingen – *A Descriptive Catalogue of the Royal Victoria and Albert Gallery of Etchings*. Kjøpere av katalogen ville også få en kopi av dronningens eller prinsens signatur, kopiert fra raderingene. Katalogen omfatter 63 raderinger. Katalogen ble innledet med en betraktning over den offentlige interesse som knyttet seg

til arbeidene. Det ble fremhevet at utstilling katalogen viste til, ville gjøre at enhver kunne danne seg en mening om dronningens og prinsens evner, der var, som katalogen vedgikk, vanskelig å briljere som billedkunstner, til og med vanskelig å heve seg over det middelmådige. Det ble trykket 51 eksemplar av katalogen, deretter ble blysatsen brutt opp.

Strange klaget til visekansleren, Knight Bruce, for å få den midlertidige beføyelsen opphevet. Han sa at etter at han var blitt kjent med prinsens innvendinger, så ville han ikke utgi katalogen. Men siden han hadde full rett til å gjøre det, burde beføyelsen oppheves. Visekansleren avslo begjæringen, og Strange henvendte seg til Lord Chancellor, Cottenham. Han avslo klagen med den begrunnelse at opplysningene i katalogen måtte være ulovlig innhentet «in breach of trust, confidence or contract». Lord Cottenham sa at «privacy is the right invaded», og konkluderte med at ettersom dronningen og prinsen hadde laget raderingene for sin egen personlige bruk, var de berettiget til å hindre offentliggjøring og bestemme hvorvidt og eventuelt hvem som skulle få tilgang til dem.

Til tross for at avgjørelsen viser til et knippe prejudikater, bl a *Wyatt v Wilson* (1820) som angikk en gravering av kong George III på dødsleiet, anses den som den første avgjørelsen som fastslår at det i engelsk rett finnes et personvern.

2 «Hvo, som krænker Privatlivets Fred …»

Hovedbestemmelsen om vern av privatlivets fred i norsk rett er straffeloven § 390: «Med bøter eller fengsel inntil 3 måneder straffes den som krenker privatlovets fred ved å gi offentlig meddelelse om personlige eller huslige forhold.» Bakgrunnen for denne hovedbestemmelsen er uklar.

I arbeidet med å lage en alminnelig straffelov, ble den daværende «Lov angaande Forbrytelser af 20de August 1842» revidert ved en omfattende endringslov av 29.6.1889. Ved denne endringen ble det inntatt en bestemmelse som er forløperen til straffeloven § 390:

> *«Hvo, som krænker Privatlivets Fred ved uden paavislig agtverdig Grund at give offentlig Meddelse om personlige eller huslige Forhold, straffes med Bøder eller Fængsel.»*

Som Ole Tokvam har vist i *Personvern og straffeansvar – straffeloven § 390* (CompLex 4/95, Tano, Oslo 1995) var denne endringen ikke medtatt i det opprinnelige forslaget. Det dukket først opp i utkastet til ny straffelov, «Straffelovkommisisionens Udkast til forskjellige kapitler i Straffelovens specielle del». I den opprinnelige forslag av 15.5.1888 mangler bestemmelsen, og

den er klemt inn mellom §§ 4 og 5 i kapittel 14 om ærekrenkelser med betegnelsen § 4a, den eneste bestemmelsen som har en slik «bokstavbenevnelse». I innstillingen til Odelstinget (Indst O VI for 1889 s 25) er det en svært knapp begrunnelse på ett avsnitt, hvor det henvises til «den danske Strafelov af 10de Februar 1866 dens § 220 og flere fremmede straffelove». Hvilke fremmede lover det gjelder, fremgår ikke av motivene, og det har ikke lykkes å finne frem til hvilke det siktes til. Forarbeidene fremhever dessuten at bestemmelsen er ønskelig «Under Forholdenes Udvikling ogsaa hos os».

Hvilke forhold det siktes til, blir altså ikke presisert. I *Lov&Data* 89/2007:18-19 diskuteres den skjellsettende artikkelen til Samuel D Warren og Louis D Brandeis i *Harvard Law Review* 1890: «The Right to Privacy». Denne artikkelen kommer altså nesten samtidig som den norske lovendringen, og den tar utgangspunkt i «øyeblikksfotografier og avisskriverier». Sammenfallet i tid kan lede til den hypotese at det nettopp var utviklingen i bruk av media og kunstneriske fremstillinger som også var foranledningen til den norske lovendringen. Norge manglet nok dagsaviser med en aggressivitet som svarte til de amerikanske eksemplene, men man hadde hatt offentlig debatt om f eks romanene Hans Jæger *Fra Kristiania-bohemen* (1885) og Kristian Krogh *Albertine* (1886). Diskusjonen berørte også forholdet til mulige levende modeller – ikke minst gjaldt dette Jægers roman, hvor hovedpersonen Jarmann blir ansett for å være en lett forkledd versjon av hans venn Fleischer, og Fleischers selvmord ble satt i forbindelse med boken. Dette er også den hypotese Ole Tokvam fremmer i sin avhandling.

I forbindelse med markeringen av Det Norske Videnskaps-Akademis 150 år har O Henrik Akeleye Braastad utarbeidet en fremstilling om «Kjærlighetshistorien bak Akademiets hus», som fremstillingen nedenfor i det alt vesentlige bygger på.

De fleste vil kjenne det store, gule paleet på Drammensveien 78 i Oslo, som også har vært rammen for nordiske konferanser i rettsinformatikk. Huset ble reist av Hans Rasmus Astrup, han flyttet 1887-88 fra Stockholm til Oslo med en stor formue, og lot arkitekten Herman Major Backer oppføre det imponerende huset – hvor han samlet fremtredende personer til en slags politisk salong. Etter hans død overdro i 1909 de to gjenlevende døtrene bygningen til Akademiet etter et forslag som var formet av familievennen og medlem av Akademiet, Waldermar C. Brøgger.

I vår forbindelse er det den eldste datteren, Ebba Mortine Marie Augusta Astrup (1863-1944), som fanger interessen. Hun vokste opp i Sverige, der faren etablerte en stor skogindustriell virksomhet – det var salget av denne som var grunnlaget for den formuen han brakte med seg til Norge. Da hun 18 år gammel besøkte London, traff hun for første gang Ole Jørgensen Richter.

Han var født i 1828, utdannet jurist, han ble stortingsrepresentant i Kristiania og i 1884 norsk statsminister ved statsrådavdelingen i Stockholm. Richters selskaplighet hadde ry for å være fornem og ekstragalant. Han var selv en vakker mann, ærekjær og følsom. Da Richters hustru døde i 1885, møttes han og den 22 år gamle Ebba i oktober samme år, og ble enige om å holde sammen. Aldersforskjellen mellom dem var 34 år. I 1887 ble Richter statsråd for offentlige arbeider og medlem av den norske statsrådsavdelingen i Stockholm. Han flyttet inn i Ministerhotellet og delte tak – selv om det var et stort tak – med Ebba. De forlovet seg i all hemmelighet 14.3.1888 og planla bryllup og et nytt liv: Kong Oscar II hadde lovet at Richter skulle bli ambassadør i London.

Omtrent på samme tid hevdet Bjørnstjerne Bjørnson – først i en tale og deretter i Dagbladet – at Richter i et fortrolig brev til ham selv hadde fortalt at statsminister Johan Sverdrup hadde løyet om sin kunnskap om en kontroversiell avtale mellom Kongen og den norske og svenske regjerning om Norges rett til likeverdig innflytelse i utenrikssaker og til en norskfødt utenriksminister i Unionen. Diskresjonen ble brutt på en uttillatelig måte og Sverdrups politiske anseelse er alvorlig skadet.

Richter uttalte at «… dette er mord – B.B. har myrdet meg på min egen fødselsdag.» Richter uteble til frokost 15.6.1888. Like etter klokken ti ble søsteren så bekymret at hun gikk opp til statsministerkontoret. Der fant hun Ole Richter død, han hadde skutt seg selv gjennom munnen. Kong Oscar II uttalte:

> *«Den som på sitt samvete har, och till sitt livs slut måste bära, skulden för Ole Richters mord, det är Björnstjerne Björnson, han och ingen annan! Han står skyldig inför Gud, og skall och stå skyldig inför historien!»*

I et langt brev til sin venn statsråd Arctander fortalte Waldermar Brøgger detaljert om selvmordet, og sa at han trodde forholdet til Ebba hadde vært avgjørende. Richters økonomi var vaklende, han var mistenkt for å søke forhold til kvinner for deres pengers skyld – og uten statsministerembetet og Kongens velvilje tillot ikke hans ære ham å fri til Astrups rike datter.

Dette var et stoff som Bjørnstjerne Bjørnson utnyttet i skuespillet *Paul Lange og Tora Parsberg* (1898), selv om han der utelot brevepisoden. I et brev til Bjørnson skrev Ebba Astrup: ”Jeg har ikke læst Deres bog, men aviserne bringer referater som sårer dybt. De bringer Deres pæn til en grusom gjerning …» Samme dag skrev hun til sogneprest Thorvald Klaveness, kjent bl a som en av grunnleggerne av tidsskriftet *Kirke og Kultur:*

> *«Det er Bjørnsons nye bog i sin raa hensynsløshet som gjør mig saa fortvilet. Har han rett til å omdanne og fremstille saa som det passer ham? – at*

bruge hvilke midler som helst – bare til sit eget øiemed? Findes der ingen grænser? Og har mennesker ret at tage mod Denne bog som et andet stykke 'kunstværk' – til at nyde medmenneskers sjelekvaler, sorg og jammer som kunstværker --? Det er for umenneskelig grusomt.»

Åpenbart var skuespillet *Paul Lange og Thora Parsberg* etter Ebba Astrups syn nettopp et eksempel på at privatlivets fred ble krenket ved at Bjørnson "uden paavislig agtverdig Grund". Men skuespillet ble offentliggjort først i 1898, lenge etter at Straffelovkommisjonens forslag til § 4a ble vedtatt. Imidlertid ble endringsloven i tid forberedt og vedtatt nær opp til Ole Richters selvmord.

Nå er det vanskelig å hevde at Bjørnsons omtale av den hemmelige avtalen mellom regjering og konge var en offentliggjørelse av opplysninger om «personlige eller huslige Forhold». Det taler derfor mot at det var denne episoden alene som foranlediget det plutselige endringsforslaget. Men likevel synes episoden å kaste lys over hva det siktes til når forarbeidene mer generelt snakker om «Forholdenes Udvikling ogsaa hos os». For saken kommer jo nesten samtidig med Jægers og Kroghs romaner. Sammenfallet i tid med artikkelen til Warren og Brandeis i USA, og den uspesifiserte henvisningen til «fremmede straffelove», synes å antyde at det var en form for internasjonal debatt om utnyttelsen av folks privatliv som stoff for aviser, romaner mv.

Likevel er de nærmere forholdene rundt begrunnelsen for Straffelovkommisjonens forslag til § 4b uklare, og vil fortsatt kunne egge til nærmere undersøkelser av bakgrunnen for denne første eksplisitte personvernbestemmelsen i norsk rett.

3 Balladen om den røde kimono

Dommen om «To mistenkelige personer» (Rt-1952-1217) slo fast at det fantes et ulovfestet personvern i norsk rett – en dom som er et hovedeksempel på Høyesteretts rettsskapende virksomhet. Bakgrunnen for dommen er tidligere omtalt i *Lov&Data,* særlig Per Jørgen Ystehede «'To mistenkelige personer' – blad fra norsk kriminalhistorie i et idéhistorisk perspektiv» *Lov & Data* 89/2007:1-6.

Forut for dommen ble professor Johs Andenæs bedt om å utarbeide en betenkning, *«Juridisk utredning om filmen 'To mistenkelige personer'»* ble senere (mye senere) utgitt i CompLex 5/95, Tano, Oslo 1995. I betenkningen

gjennomgår Andenæs utenlandsk rett, og finner bl a frem til den amerikanske dommen *Melvin v Reid (Gabrille Darley Melvin v Dorothy Daveport Reid, District Court of Appeal, Fourh District, California 28.2.1931*). Dommen er altså i år 70 år gammel.

I følge Andenæs fremstilling, gjaldt saken en tidligere prostituert kvinne, Gabrielle Darley som i 1918 ble tiltalt for mord, men frifunnet. Hun la sitt gamle liv bak seg, og giftet seg med Bernhard Melvin og var ikke lenger kjent under sitt tidligere navn. I 1925 ble det laget en film med tittelen *The Red Kimono Case,* bygget over hennes liv. Her ble hennes pikenavn brukt, og i omtalen ble det angitt at det var en sann historie. Dette førte til at hun ble utsatt for forakt av sine nye venner, og hun anla sak mot selskapet med krav om erstatning.

Retten fant at det ikke var en personvernkrenkelse. «The very fact that [these incidents] were contained in a public record is sufficient to negative the idea that their publication was a violation of a right of privacy.» Hvis det forelå noen krenkelse, var den begrunnet i at saksøkers virkelige navn ble brukt sammen med hendelser fra hennes liv. Retten fant at en slik krenkelse forelå ettersom Californias konstitusjon art I sikret borgere retten «to pursue and obtain happiness».

Andenæs avslutter sin omtale av saken med å påpeke forskjeller mellom denne og den norske saken.

Journalisten Leo W Banks har sett nærmere på historien om Gabriell Dardley – skrivemåten er avvikende fra den som brukes i dommen, her brukes dommens skrivemåte. Denne gjenfortellingen er basert på hans artikkel «Muderous Madam», *Tucson Weekly* 6.5.2000.

Drapet som var utgangspunktet for saken mot Darley, skjedde 1.1.1915 på West Seventh Street, Los Angeles. Gabrielle Darley var kledd i silke og pels da hun gjennom vinduet til en spritbutikk så Leonard Topp. Han hadde vært hennes hallik, og gjentatte ganger lovet å gifte seg med henne – men han giftet seg med en annen, og stjal fra henne en liten formue i diamanter. Hun gikk inn i butikken og skjøt ham. Han klarte imidlertid å slå henne sanseløs før han selv døde. Saken skapte store overskrifter. I *Los Angeles Evening Herald* var det den 21 år gamle reporteren Adela Rogers St Johns som dekket begivenheten, hun var kjent som en «sob sister», en journalist som skulle får leserne til å gråte:

> *«In her blood pulses the forces of fiery love and quick revenge. And in her wonderful gold-green eyes, fire flashes as she calls for her sweetheart – calls again and again, unaware that she is calling across the gulf of an open grave.»*

Påtalemyndigheten ved District Attorney William C. Doran mente saken var opplagt. Forsvarer var Earl Rogers, faren til den unge journalisten og en av de mest kjente straffeadvokater i sin tid. Han var fargerik, det het seg at han brukte fritiden til å drikke og feste i byens bordeller, men at han etter noen timer i et tyrkisk bad på ny var klar for skranken. Darley kunne ikke betale salæret hans, men Rogers tok saken fordi den var høyt profilert, og fordi ha hadde en affinitet for «sporting girls». Det fortelles (av Alfred Cohn og Joe Chisholm *Take the Witness!*, 1934) at økonomien ble løst da en eldre dame kom til Rogers kontor dagen før rettssaken. Hun sa hun en gang også hadde arbeidet på en bordell, men nå var respektabel. Hun hadde ikke mye penger, sa hun, men ga Rogers en sigarboks med juveler som han pantsatte for 3 000 dollar.

For rettssaken valgte Rogers en taktikk som ikke før var prøvd. Han fikk galleriet i rettssalen fylt av overklassekvinner som sympatiserte med Darleys skjebne – frelsesarmesoldater i full uniform, prestekoner og sirlige filantroper som holdt rundt blomsterbuketter og gispet over hvert nytt argument som sjokkerte dem. Rogers hadde også overtalt en berømthet til å være til stede, sopranen Ellen Beach Yew, kjent som Californias sangfugl.

Gabrielle Darley fortalte journalister om sin skjebne. Hun var født i Berganda, Italia – familien flyttet til New York da hun var ett år gammel. Faren forsvant da hun var åtte, moren og hun selv måtte flytte til San Francisco hvor moren arbeidet som sydame, og hun selv måtte hjelpe til og derfor ikke fikk skolegang. Moren forsvant i forvirringen etter jordskjelvet i 1906. Bare 16 år gammel slo hun seg sammen med en eldre kvinne og dro mellom byer og leire for gullgravere. Hun møtte sin første ektemann da hun var servitrise ved en restaurant i Las Vegas, men han ble skutt to år senere – igjen var hun alene.

Dette var stort sett et eventyr. Gabrielle Darley var født i Frankrike omkring 1890, og kom til USA som tenåring for å arbeide som hushjelp hos et italiensk ektepar.

Forsvareren fremstilte Leonard Topp som en elegant og vakker bartender med et godt øye til slipsnåler og mansjettknapper med diamanter, som han betalte for med andres penger. Han pantsatte Gabrielles juveler og forfalsket sjekker i hennes navn. Hun trodde på løfter om ekteskap, og kjøpte diamantringer til ham for å gjøre ham til lags. Men han solgte bilen hennes, brukte opp pengene hennes og banket henne to-tre ganger i uken.

Juryen besto bare av menn. Det tok den åtte minutter å frifinne Gabrielle. Juryens formann uttalte til pressen at hun hadde rettet opp den urett hun hadde vært utsatt for. I St Johns memoarer (1962) heter det at når det gjelder menn som Leonard Topp, kan ikke bare drap rettferdiggjøres, det må være en kvinnes forpliktelse.

Fra filmen The Red Kimono

Gabrielle ble tatt rett fra fengselet til Yews villa for å tilbringe noen uker i velstand. Hun erklærte at hun var et nytt og bedre menneske, og at hun ville bli sykepleier.

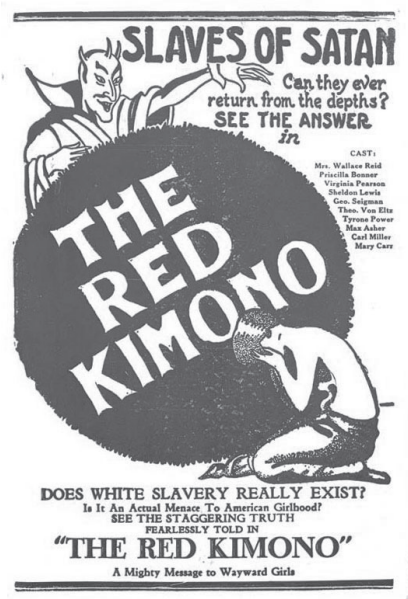
Dette var noe av den faktiske bakgrunn for filmen *The Red Kimono* (1925). Kvinnen bak filmen var Dorothy Davenport Reid (1985). Hun debuterte som filmskuespiller da hun var 16 år, og spilte sammen med Wallace Reid i en western, *His Only Son.* De laget en rekke filmer sammen, gjerne to i uken. De giftet seg i 1913.

Wallace Reid ble berømt som smeden med naken overkropp i *The Birth of a Nation,* og han ble stadig mer populær, ekteparet flyttet inn i et hus på Sunset Boulevard som det heter at var det første filmstjernehuset med svømmebasseng. I 1919 ble Wallace Reid skadet av et tog i en ulykke under en filminnspilling. Han smertene vedvarte etter at han ellers ble frisk. Han fikk morfin, og ble avhengig av det. Han døde av en overdose i 1923, bare 31 år gammel.

Dorothy Reid ble deretter en aktiv motstander av narkotika. Sammen med Adela Rogers St John til en konferanse om stoffmisbruk i Washington DC, og hun laget sin første film, *Human Wreckage,* som ble en stor suksess.

The Red Kimona var den tredje i rekken av filmer begrunnet av hennes sosiale samvittighet, og handlet om prostitusjon. Adela Rogers St Johns novelle ble bearbeidet for film av Dorothy Arzner – som senere sto frem som lesbisk, og som ble en pioner i feministisk film. Filmens navn har – i likhet med navnet til Gabrielle Darley – flere versjoner, i dommen omtales den som *The Red Kimono,* men flere kilder kommenterer den merkelige stavemåten.

Filmen ble distribuert nasjonalt, og fikk en blandet mottakelse. Den ble også februar 1928 vist i Elks Theatre, Prescott. Gabrielle Darley var på denne tiden eier av Mason Hotel like i nærheten, hvor hun huset gatepiker. Ved inngangen til kinoen satt en voksdukke kledd i en rød kimono. Gabrielle Darley satte seg



uten å ane at det var hennes egen livshistorie som lå til grunn for filmen.

Men det ble snart klart nok. I begynnelsen vises Dorothy Reid mens hun leser avisreportasjen fra 1917 – som avsluttes med at hun ber om forståelse for denne «Modern Magdalen». Filmen bruker også Gabrielle Darleys eget navn.

Snarere enn å akseptere det nokså tiltalende portrettet filmen gir av henne, saksøkte hun Dorothy Reid og Diamond All-Sttar Features Distributors Inc i juni 1928. Hun hevdet at hun etter 1915 hadde levd et eksemplarisk liv, og at filmen ga en offentlig fremstilling av hennes som «a woman of lewd characteristics, a prostitute and a murdress», noe som ydmyket og påførte henne dyp sorg, smerte og tap av selvrespekt. Det ble også hevdet at bruk av navnet hennes krenket hennes eiendomsrett til dette. Kravet var på 50 000 dollar i erstatning.

Saken ble kastet frem og tilbake i Californias rettssystem i fem år. Statens høyesterett ville ikke realitetsbehandle anken, det vil si at appelldomstolens avgjørelse ble stående. Dorothy Reid inngikk et forlik som praktisk talt slukte alt hun eide, inklusive det mye omtalte huset med svømmebasseng. Hun gikk personlig konkurs i 1933.

Lee W Banks forteller at Gabrielle Darley etter denne seieren for domstolen fortsatte å leve som hun var vant til. Han reflekterer over skjebnen til de menn som krysset hennes vei – seks menn som enten ble skutt, forgiftet eller døde under mystiske omstendigheter. Han antyder at det kan ha vært flere. Hun var innblandet i nye rettssaker, den siste en drapssak fra 1962 der eieren av en bensinstasjon skjøt og drepte en mann. Gabrielle Darley tok initiativ til å dekke utgiftene til en dyktig forsvarsadvokat. Siktede ble frifunnet, men fem dager etter dommen havnet Gabrielle Darley på sykehus med brukket hofte og lungebetennelse. Hun døde juledag 1962.

4 Bare et nummer …

Vi har alle et navn. Like etter at vi fødes, får vi et navn – gjerne ledsaget av en dåp som understreker at dette er en viktig begivenhet. Vi identifiserer oss med

navnet – det er ikke bare en betegnelse på oss, men nærmest en del av oss. I nordisk tradisjon er faktisk navnet viktigere enn i mange andre tradisjoner, noe som f eks speiler seg i at vi har beskyttede slektsnavn.

Men vi har også alle sammen et nummer. Dette er et entydig nummer som de fleste av oss får ved fødselen. Det er bygget opp på en finurlig måte, utviklet av professor Ernst Selmer. De seks første sifrene angir fødselsdato (ddmmåå). De tre neste sifrene har flere funksjoner: For det første er det et løpenummer som skiller fra hverandre de som er født samme dato. For det andre angir det kjønn – oddetall for menn, liketall for kvinner. Og for det tredje angis det århundre man er født i. De to neste tallene er kontrollsiffer – det tiende tallet beregnes på grunnlag av de ni foregående tallene, det ellevte begrenes på grunnlag av alle de foregående tallene. Dette betyr at tallet er selvverifiserende, ved å utføre de to små regnestykkene, kan man bestemme at tallet er «gyldig», en mulighet som for øvrig utnyttes alt for sjelden.

Hele tallet kalles «fødselsnummer» (fordi det har med fødselsdatoen), mens de siste fem tallene kalles «personnummer». Hver av oss har altså et unikt fødselsnummer, selv om vi skulle ha et samme dåpsnavnet, eller være født på samme dato. Det fremstår vel som åpenbart at det er fordeler ved på denne måten sikkert å kunne identifisere ulike personer, og å unngå sammenblanding. Men det er svært få land som har innført et slikt system – bare en håndfull, selv om det enkelte steder er tatt i bruk nummer som er tildelt for andre formål mer generelt: I USA er det utstrakt bruk av «social security number», i Canada brukes det tall som anvendes i skatteadministrasjonen på lignende måte.

> *Social Security number 078-05-1120 har en spesiell historie. En produsent av lommebøker brukte i 1930-årene sekretærens nummer på et kort som ble lagt inn i lommebøkene for å vise hvordan det kunne få plass. Kortet var merket med «specimen», men utallige kjøpere trodde likevel at det var nummeret de var tilordnet. Titusener av dollar ble overført til kontoen, og det tok over tyve år å løse problemet. Sekretæren fikk et nytt nummer – eller ville hun ha fått millioner av dollar i pensjon.*

Mange assosierer fødselsnummeret med datamaskinbaserte systemer, men begrunnelsen for innføringen finner man i andre hensyn. Opprinnelig ble det brukt ulike nummerserier for næringslivets rapportering av opplysninger til offentlig forvaltning – et eget nummer for trygd, skatt osv. Dette skapte behov for å holde orden på en lang rekke nummer f eks for ansatte – og det vokste frem et krav om forenkling. Kravet fikk tilslutning fra Statistisk sentralbyrå, som så muligheter for forbedring av offentlig statistikk. I 1961 fikk SSB i opp-

drag fra Finansdepartementet å utrede spørsmålet om et fast identifikasjonsnummer, og innføre dette om det viste seg mulig. Dette skjedde i oktober 1964.

I ettertid fremstår det kanskje som noe overraskende at dette skjedde som et rent administrativt tiltak for forenkling av kommunikasjon mellom privat og offentlig sektor. Stortinget hadde ikke noe med innføringen å gjøre bortsett fra at Det sentrale personregister er med som en budsjettpost i statsbudsjettet for 1963 og senere år. Lovhjemmel fikk man først i 1970. Det var heller ingen debatt om innføringen – noe som igjen kan oppleves som overraskende når man vet hvilken politisk motstand som tilsvarende forslag i f eks Tyskland og Nederland vakte senere. Fødselsnummeret ble ledsaget av etableringen av Det sentrale personregister, som angir grunnleggende opplysninger om den enkelte (som adresse, arbeidsgiver mv), og knytter den enkelte til foreldre, ektefelle og barn.

Fødselsnummeret ble altså innført for å forenkle manuell administrasjon. Hadde man hatt datamaskiner på dette tidspunkt, ville det ikke vært et så stort problem å administrere ulike nummerserier overfor ulike myndigheter. Og effektiviteten ved å bruke fødselsnummer for å samkjøre registre sammenlignet med bruk av f eks fødselsdato og navn, er ikke mer en et par prosent. Mange land med større befolkning enn Norge (f eks England) klarer seg uten et slikt nummer, nettopp fordi man i dag har datamaskinbaserte systemer.

Likevel er fødselsnummeret blitt et slags symbol på at man er «redusert til et nummer» i den offentlige forvaltning. Det overrasker mange at fødselsnummeret ikke er taushetsbelagt (jfr forvaltningsloven § 13, 2.ledd), dvs. at man på henvendelse til folkeregisteret kan få opplyst en persons fødselsnummer. Men personopplysningsloven § 12 har likevel særlige regler for bruken – dette bygger nok nettopp på at mange oppfatter nummeret som noe mer enn et «navn», nærmest som en nøkkel til mange registre i offentlige og private registre.

Og denne alminnelige følelsen kommer vel nettopp av uviljen mot «bare» å bli behandlet som et nummer. Jeg har forsøkt å finne den tidligste referansen til dette. Og en kandidat er Eugen Samjatins utopiske roman *Vi* (1920, oversatt til norsk av Alf Biem). Samjatin spilte en ledende rolle i Moskvas litterære liv de første revolusjonsårene. Men han ble snart skremt av utviklingen, og skrev *Vi* som et brudd med sin fortid. Boken ble ikke trykt i Sovjet, men et manuskript ble smuglet ut og trykt i utlandet. Samjatin kritiserte Stalin, bl.a. i et åpent brev fra 1931. Til tross for dette, og muligens på grunn av sitt vennskap med Maxim Gorkij, fikk han utreisetillatelse samme år og slo seg ned i Paris, hvor han døde i 1937.

Vi er en betydelig roman, som har spilt en rolle både for Huxleys *Brave, New World* (1932) og Orwells *1984* (1949). Og i Samjatins fremtidsstat er individualitet forsøkt fjernet, mennesker skal ikke tenke på seg selv som «jeg», men som «vi», og derfor har de ikke lenger navn, bare nummer … Likevel blir hovedpersonen D-503 forelsket i den merkelige kvinnen I-330.

Kanskje noe av fødselsnummerets symbolverdi henger sammen med denne boken? Eller har det den mer hverdagslige forklaringen av fødselsnummeret vekker forestillingen om at vi alle lik soldater blir identifisert med nummer, som den rulleførende enhet – staten – bruker når den henvender seg til oss.

5 Biometri: Fingeravtrykk og Pudd'nhead Wilson

Sir Williams fingeravtrykk (etter Galton)

Læren om fingeravtrykk kalles daktyloskopi, og omfatter bruk av fingeravtrykk til å identifisere f eks forbrytere. I 1877 tok Sir William James Herschel i bruk fingeravtrykk til identitetskontroll i fengslene i Bengal, India. Men det var først da han sammen med Henry Fauld i 1880 skrev den berømte artikkelen i *Nature,* at dagens metoder for bruk av fingeravtrykk ble foreslått. Francis Galtons bok *Finger Prints* (1892) systematiserte kunnskapen.

Ved en lovendring av 2005:93 ble det gjort en endring i passloven (1997:82) § 6, 2.ledd som nå bestemmer at til «bruk for senere verifisering eller kontroll av passinnehaverens identitet, kan det innhentes og lagres i passet biometrisk personinformasjon i form av ansiktsfoto». Dette er på en måte en passende markering av at det er 100 år siden fingeravtrykk – det første eksempelet på biometri for praktisk bruk – ble introdusert i Norge. Kort tid senere ble Kristiania Kriminalpolitis Signalementkontor åpnet (1906) i Møllergaten 19.

Nedenfor bringer vi litt fra fingeravtrykkets historie i forbindelse med en kommentar om HG Wells roman *A Moderen Utopia* (1906), som foreslo en europeisk fingeravtrykksentral som del av det system som skulle gjøre det mulig å reise fritt på tvers av datatidens mange grenser, en slags tidlig forløper til Schengen-avtalen.

Den første fellende dom i Norge med fingeravtrykk som eneste bevis, ble avsagt 14.10.1910. Da hadde de for lengst erobret kriminallitteraturen. Den første av disse er skrevet av Mark Twain.

Mark Twain – illustrasjon til forordet «A Whisper to the Reader»

Pudd'nhead Wilson er en slags sørstatsroman, lagt til den søvnige småbyen Dawson's Landing på Missouri-siden av Mississippi, en halv dags ferd med dampbåt nedenfor St Louis. En dag i 1830 flytter en ung advokat til byen, David Wilson. Han gjorde et uheldig førsteinntrykk – mens han sto og snakket med et par av byens borgere første dag i byen, ble de forstyrret av gjøingen fra en bikkje. Wilson kom til å si:

«Jeg skulle ønske jeg eide halvparten av den bikkja.»

Og da han ble spurt om hvorfor det, svarte han: «For da kunne jeg ha drept min halvpart.»

Byens borgere mente dette var en uklok manns tale. For hadde han tenkt på hva som ville skjedd med den andre halvparten om han drepte sin? Tydeligvis ikke. Dermed fikk han oppnavnet «Pudd'nhead», som han ikke ble kvitt før i slutten av romanen.

Egentlig er hovedpersonen en annen, Thomas à Beckett Driscoll, sønnen til en rik plantasjeeier. Han hadde en barnepike, Roxy, som hadde en jevnaldrende sønn, Valet de Cambers. Roxy var neger og slave, hun hadde like lys hudfarge som andre, men «the one-sixteenth of her which was black outvoted the other fifteen parts and made her a negro». Hun passet på de to guttebarna, som lignet så mye på hverandre at faren hadde vanskelig for å se forskjell på dem. Og da plantasjeeieren en dag truer med å selge slavene sine «down the river» som straff for at noen av dem hadde stjålet noen penger, kler

hun Chambers i den snøhvite barnekjortelen med blå sløyfer og blonder som tilhører Thomas, som selv får striskjorten til hennes egen sønn. De blir forbyttet, og vokser opp forbyttet – Thomas viser seg å bli en dugende arbeider, mens Chambers blir en overklasseslamp.

Men før forbyttingen har Wilson forfulgt sin store lidenskap. Han har tatt barnas fingeravtrykk:

> *«I jakkelommen hadde han en smal boks med spor inni, og i sporene var det striper av glass fem tommer lange og tre tommer brede. Nederst på hver stripe var det klistret et stykke hvitt papir. Han ba folk dra fingrene gjennom håret (slik at de fikk på seg et tynt lag naturlig olje) og så trykke tommelen mot glasset, deretter hver av tuppene på de andre fingrene etter tur. Under denne raden med avtrykk skrev han et notat på det hvite papiret – slik: 'John Smith, høyre hånd –'»*

Historien som utvikler seg, skal vi ikke gå nærmere inn på. Det får være tilstrekkelig at Chambers (som alle tror er Thomas) kommer i spillegjeld, og stjeler penger for å dekke denne. Han blir overrumplet da han forsøker å stjele fra sin sovende gudfar, og dreper ham med en indisk dolk han tidligere har stjålet fra noen tilreisende italienske tvillingbrødre. Brødrene får skylden, alle indisier peker mot en av dem (men tvillinger er som hunder, man kan ikke bare henge den ene). Men dolken er funnet ved den myrdede, og i blodet er det klare fingeravtrykk.

Wilson forsvarer de tiltalte brødrene. Og i en stor tale som Twain har formulert med sin mesterlige sans for ironi, prosederer han sin sak:

> *«Og denne dolk er signert med morderens medfødte autograf, skrevet i blodet til den hjelpeløse og sakesløse mann som elsket dere og dere alle elsket. Det er bare ett menneske på hele Jorden med en hånd som kan kopiere dette blodrøde tegnet, og den gode Gud vil vise oss dette menneske før klokken slår middagstimen.»*

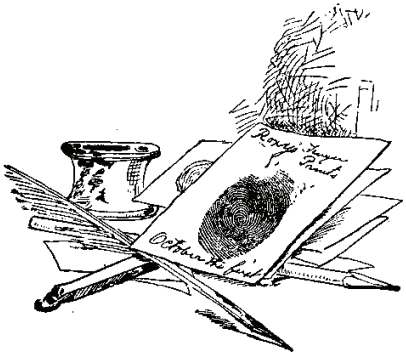
Wilson demonstrerer at fingeravtrykk er unike ved å få forsamlingen til å presse hendene mot vindusrutene. Han oppklarer mordet, og samtidig forvekslingen av de to guttebarna. Chambers er igjen slave, og blir krevd utlevert av kreditorene til dekning for sin gjeld.

Slik ender altså verdens første kriminalbok der fingeravtrykk ble brukt som bevis, og slik mistet Wilson sitt kallenavn «Puddn'head». Men bak denne overfladiske intrigen i romanen lurer det viktigere spørsmål – om farget og hvit, om slaver og slaveeiere, om berettigelsen av det systemet som Sørstatene

romantiserte: En kritiker har kalt romanen en «parable of property» (Georg M Spangler, *American Literature* mars 1970).

Handlingen er altså lagt til 1830, men kunnskapen om fingeravtrykk som bevis for identitet Twain, ble først kjent ved utgivelsen av Francis Galton *Finger Prints* (1892), og det førte til at Twain reviderte fortellingen og innførte Wilson som hovedperson i oppklaringen av mordet. Boken ble utgitt som føljetong forut for bokutgivelsen, den første delen trykt i *Century Magazine* desember 1893. Twain var altså på mange måter en mann forut for sin tid, en demonstrasjon er hans «omvendte» science fiction-roman *Connecticut Yankee in King Arthur's Court* (1889).

Kapitlene i *Puddin'head Wilson* inneholder utdrag av en «kalender» Wilson skal ha skrevet – ett av disse visdomsordene kan passende avslutte denne lille fotnoten til biometriens historie: «Bemerkning om oppkomlinger: Vi vil ikke serveres sopp som tror de er trøfler.»



Illustrasjon til kapittel 4

6 Et moderne utopia

I et Europa uten grenser oppstår det er behov for å erstatte den rutinemessige kontroll med mennesker bevegelser ved grensen med en annen form for kontroll. I kjølvannet av Schengen-avtalen som avskaffet grensekontroll mellom flere europeiske land, så man det nødvendig å etablere et mer effektivt samarbeid mellom landenes politimyndigheter med sikte på gjensidig hjelp ved å lokalisere en ettersøkt person og andre kontrolloppgaver. Dette samarbeidet skulle organiseres rundt et datamaskinbasert system, SIS

(for «Schengen Information System»), og løsningen er arvet av Den europeiske unions indre marked.

Et slikt samarbeid mellom mange land med sikte på kontroll med enkeltpersoner, reiser naturligvis mange spørsmål relatert til personvern. Men det er også kuriøst å oppdage at problemstillingen ikke er ny.

Et hovedproblem er å knytte en sikker identifikasjon til enkeltmennesker - det som ofte kalles problemet med *autentifikasjon*, sikkerhet for at en identifisert person også virkelig er den hvis identitet vedkommende benytter. Vi er vant til at fingeravtrykk er en sikker måte for autentifikasjon. Den første virkelige utførlige bok om fingeravtrykk var Francis Galton *Finger Prints* (1892). Det første offisielle fingeravtrykksbyrå ble etablert i La Plata i 1891, og benyttet sammen med andre biometriske målinger, og ble som eneste metode innført i Storbritannia 1901, Tyskland og USA 1903, Danmark 1904 og Sverige 1906. I Norge kom fingeravtrykk i praktisk bruk fra høsten 1905, og ble offisielt innført 1.1.1906 ved åpningen av Kristiania Kriminalpolitis Signalementkontor.

Rundt århundreskiftet var altså nettopp fingeravtrykk en nyhet. Og det er derfor ikke spesielt overraskende at HG Wells benytter dette prinsippet i sin «roman» (for den er kanskje mer et animert essay) *A Modern Utopia* (1906).

HG Wells skrev denne fremtidsvisjonen i et Europa hvor reise mellom land var en omstendelig affære som ofte krevde tillatelser, pass og visa. Slik kunne det ikke være i et moderne utopia, mente han - hele verden ville «fylles av anonyme fremmede», så «flytende som flo og fjære». I denne verden hvor «fri flyt av personer» var innført, kom tollovgivningen og andre gjeldende metoder fra Wells samtid til kort, og han foreslår innføring av et nytt system som «raskt og sikkert kan identifisere ethvert menneske i verden».

Wells anså dette slett ikke for å være noen umulig oppgave. Han tenkte seg en katalog over alle Jordens innbyggere lokalisert «i en rekke store hus i eller nær Paris». Katalogen ville være sortert etter klassifikasjon av fingeravtrykk, og på dette grunnlag kunne vært individ tilordnes «en bestemt formel, et tall eller 'vitenskapelig navn'» - muligens er dette første gangen tanken om et universelt personnummer blir formulert.

Systemet tenkte Wells seg basert på indekskort - og hullkort var allerede oppfunnet ved århundreskiftet. Den nærmeste foranledningen hang sammen med den amerikanske konstitusjon som krevde at stemmer ved presidentvalget skulle fordeles på distrikter relativt til befolkningen. Dette krevde forholdsvis aktuelle folketellingstall, og i slutten av forrige århundre innså man at tiden for å telle opp resultatene av folketellingen snart ville overstige fire år. Man arrangerte derfor en konkurranse, og Herman Hollerith vant denne med sitt elektriske tabulasjonssystem basert på hullkort. I 1896 dannet han Tabulating Machine Company som ble solgt i 1911 og fusjonerte med andre selskaper som ble samlet under ad-

ministrasjon av Thomas J Watson i 1914, og ti år senere omdøpt til International Business Machines (IBM). Det er i seg selv nokså kuriøst at utviklingen av datamaskinen fikk et alvorlig puff fremover av den amerikanske grunnlov.

Men det var ikke kjedelige hullkort av kartong Wells tenkte seg at ville brukes i hans globale befolkningsregister. Han tenkte seg at kortene var gjennomsiktige slik at man kunne lage fotografiske kopier av dem når man måtte ønske, og de skulle ha et vedlegg hvor man kunne skyve inn en lapp med navn på det sted hvor vedkommende sist var observert. For en hær av mennesker var nødvendig for å vedlikeholde registeret med opplysninger om fødsler, dødsfall, hotellregisteringer, henvendelser til postkontor for brev, billetter for lange reiser, straffedommer, giftemål, søknad om sosial støtte osv. Wells så for seg hvordan et filter av kontorer sorterte strømmen av meldinger, og hvordan natt og dag saksbehandlere svermet rundt registeret for å korrigere sentralregisteret, og fotografere det for å sende kopier videre til lokalkontorer.

Wells var faktisk ikke helt fremmed for tanken at man kunne ha motforestillinger ved en slik omfattende registrering. Enkelte, medga han, ville hevde at det var deres rett å reise uidentifisert og i hemmelighet hvor man måtte ønske. Wells pekte på at dette kunne man fremdeles gjøre i forhold til sine medpassasjerer - men ikke i forhold til den nye, utopiske staten. Og Wells viftet motforestillingene til side som «vanetanker fra en ond tid», for liberalt tenkende mennesker fryktet det tyranni som lurte bak enhver av hans samtidig stater. Men dette var unødvendig i det nye utopia, hvor kunnskap om enkeltmennesket ikke ville bli misbrukt.

Gjensyn med Wells utopi fra 1906 demonstrerer forfatterens evne til å gripe ny teknologis muligheter - eksemplifisert ved fingeravtrykket og hullkortet - og projisere dem inn i en sosial dimensjon. Riktignok er visjonen av de store kontorbygningene i Paris, fylt av krystallklare indekseringskort og travle funksjonærer, alderdommelig. Men hvis man etablerer Schengen Information System etter planen i Strasbourg, ville det ikke være upassende å reise spørsmålet om hvorvidt dette faktisk er et skritt på veien mot realisering av Europas nye utopia. Og bak det spørsmålet lurer et alvorligere problem, nemlig om samfunnet i Wells visjon faktisk er et utopi - eller noe mer foruroligende, et omriss av det gjennomkontrollerte samfunn.

6.1 Når maskinen stopper

Men Wells utopi opphisset en annen engelsk forfatter, EM Forster, som skrev «The Machine stops» (1909).[1] Dette var et tilsvar til Vernes teknologioptimistiske visjon, og er i seg selv kanskje enda mer visjonær:

> *« Tenk Dem, om De kan, et lite, sekskantet rom som en celle i en bikube. Det mangler både vindu og lampe, men er likevel fylt av bløtt lys. Det er ingen instrumenter å se, likevel vibrerer rommet av melodiøs musikk. En lenestol står midt på gulvet, ved siden av den et lesebord - andre møbler finnes ikke. Og i lenestolen sitter en innhyllet kjøttklump - en kvinne - omtrent fem fot høy og med et ansikt hvitt som sopp. Det er hun som eier det lille rommet.*
>
> *En elektrisk klokke kimte.*
>
> *Kvinnen rørte ved en bryter og musikken stilnet.*
>
> *« Jeg får vel se hvem det er,» tenkte hun og satte stolen i bevegelse. På samme måte som musikken, ble stolen kontrollert av maskiner. Den rullet henne bort til andre siden av rommet hvor klokken fremdeles kimte utålmodig.*
>
> *« Hvem er det?» ropte hun.*
>
> *Det gikk femten sekunder før den runde platen hun holdt mellom hendene begynte å gløde. Et svakt, blått lys jaget over den, mørknet til purpur, og endelig så hun bildet av sønnen sin som bodde på den andre siden av Jorden. Og han kunne se henne.»*

Faktisk ble katodestrålerøret - som fremdeles brukes i fjernsynsapparater og datamaskinbaserte arbeidsstasjoner - oppfunnet i 1906.[2] Det er derfor kanskje ikke så overraskende å finne denne skildringen av et fjernsynssystem eller en billedtelefon i en novelle fra begynnelsen av dette århundre. Det som er nesten sjokkerende moderne med denne novellen er bildet den gir av et menneske

1 Sitatet er fra Bing & Bringsværd 1969:53.

2 Uavhengig kom tre beskrivelser av fjernsynssystemer basert på bruk av katodestrålerør, Max Dieckmann (tysk patent 1906), Boris Rosing (engelsk patent 1907) og Campbell-Swinton i en artikkel i *Nature* 1908.

isolert mellom kommunikasjonssystemer og media - et menneske sperret inne i et mediafengsel.

6.2 Adskillelse og møte

Fosters novelle karakteriserer to aspekter av all kommunikasjonsteknologi. På den ene siden har teknologien den virkning som er dens erklærte formål: Å bringe mennesker sammen. Telefonen gjorde det mulig for familie og venner å holde kontakt, selv om de var adskilt av geografisk avstand. Men teknologien har også en latent virkning: Den gjør det *unødvendig* å holde kontakt med den krets av mennesker som manglene av teknologien tidligere disponerte en for å ha samkvem med.

En anekdote fra Oslo illustrerer dette. Det ble hevdet av svært mange Stortingsrepresentanter i forrige århundre bosatte seg i den bydelen som kalles Homannsbyen. Årsaken var at dette gjorde det lettere å fraksjonere på kveldstid, andre representanter bodde innen gangavstand, man kunne oppsøke dem og diskutere ulike forslag og strategier. Så kom telefonen, og dermed ble ikke geografisk nærhet lenger noe vilkår for konspiratoriske samtaler på kveldstid: Homannsbyen ble frarøvet sin særlige status.

Eller ta et munnhell fra dagliglivet: I store byer er man blitt så anonyme for hverandre at man ikke kjenner sin egen nabo. Takke telefonen for det! Tidligere, om man følte seg taletrengt, var det få mulighet. Det var nærliggende å banke på naboens dør, kanskje med en unnskyldning om å få låne en kopp sukker til baksten. Så ble man invitert inn, budt en kopp kaffe, og fikk en liten prat – en helt sosialt ritual. Nå kan man i stedet ringe noen man kjenner bedre – en venn eller venninne, en kollega eller en slektning. Behovet for møte med naboer er opphørt.

Slik vil det også være med den nye informasjonsteknologien. Mange sosiale situasjoner hvor man møter andre mennesker mer eller mindre tilfeldig, vil bli avviklet. Man treffer ikke lenger folk i køer på postkontor eller andre steder man i dag må oppsøke for å få gjennomført rutinemessige gjøremål. De fleste vil oppleve det som en fordel å slippe køene. Men samtidig unngår man de tilfeldige møtene med bekjente og de påtvungne møtene med de bak skranken. Man kan håpe på at dette fører til en omvurdering av mellommenneskelig kontakt, at de fleste møter får en øket kvalitet.

Men man kan dessverre ikke se bort fra at Fosters visjon kan bli en metafor for den nære fremtid, og at man får et samfunn karakterisert av det den norske sosiologen Stein Bråten har kalt «Se og høre, men ikke røre»-samfunnet.[3]

3 Stein Bråten *Dialogens vilkår i datasamfunnet* (Universitetsforlaget, Oslo 1983).

7 Overvåking i det nittende århundre

De siste par årene er videoovervåking blitt stadig mer brukt som middel mot å redusere kriminalitet i byer og tettsteder. Ikke minst har Simon Davies – kjent som initiativtaker til Privacy International, og en forkjemper for sterkere personvern – popularisert utviklingen i England i boken *Big Brother – Britain's Web of Surveillance and the New Technological Order* (1996). Videokamera blir satt opp på lyktestolper for overvåking av offentlige gater og plasser. Enkelte steder har rapportert om oppsiktsvekkende nedgang i antallet straffbare handlinger, men tallene er kritisert av andre. Fra Norge kjenner vi foreløpig kanskje best bruk av automatisk trafikkovervåking og annen bruk av automatiske kamera i banker, postkontorer mv.

Dette er altså et aktuelt personverntema. *Lov&data* vil – som en liten bakgrunn – antyde at temaet ikke er så nytt som man skulle tro. Vi tillater oss å sitere fra en artikkel fra *The Glasgow Mechanics' Magazine* 7.8.1824. Artikkelen omhandler et *camera obscura* utstilt i markedsuken.»*Camera obscura*» betyr «mørkt rom» . De eldste versjonene stammer fra antikken, og var et lite, mørkt rom hvor lys trengte inn gjennom et eneste lite hull. Resultatet var et opp-ned bilde av scenen utenfor på den motsatte veggen, som gjerne var hvittet. I flere hundre år brukte man dette til å betrakte solformørkelser uten å risikere synet, og i det 16. århundre ble det også brukt som hjelpemiddel til å utføre tegninger: Modellen poserte utenfor, og bildet ble reflektert på et papir hvor kunstneren kunne tegne konturene. Det ble bygget portable versjoner, de ble mindre – til og med lommemodeller kom i omløp: Innsiden av esken var svartmalt og bildet ble reflektert av et skråttstilt speil slik at det kunne betraktes riktig vei. *Camera obscura* var forløperen til kameraet, og da J-N Niepce fant opp lyssensitive plater, var også fotografiet funnet opp.

Vi må anta at det var et portabelt *camera obscura* som fantes på markedsplassen i Glasgow, og hvor en bemerkelsesverdig episode fant sted:

> *« Episoden viser hvilken betydning dette underholdende optiske apparat kan få. En person betraktet interessert de ivrige skikkelsene i stadig bevegelse som ble gjengitt på den hvite tavlen. Da så han overrasket at det dukket opp en mann som stjal fra en annen manns lomme. Han forsto at dette skjedde i virkeligheten, åpnet døren, gjenkjente synderen et kort stykke unna, løp frem og grep ham på fersk gjerning. Det er kanskje unødvendig å legge til at han straks ble overlatt politiet. Av dette skjønner man lett nytten av å plassere slike apparater alle steder hvor offentligheten forlyster seg og på utstillinger. Om det ville være passende å bygge dem i gatene til folkerike byer som dette, og gi en politimann ansvar for å avdekke ugagn og lovbrudd, er noe som de lokale myndigheter bør vurdere. Ville det ikke*

være hensiktsmessig å bruke observatoriet (som ikke lenger er i bruk) som camera obscura for å observere hva som skjer i byens gater, og formidle, om nødvendig, resultatet til politiet eller fengselet ved hjelp av en telegraf? Hvis man anser at Observatoriet er for langt borte, kunne apparatet settes opp nær Tron eller Cross Steeple. Slik ville behovet for å sende ut folk for å overvåke befolkningen ville bli overflødig siden alt ville skje, så å si, under politiets våkende øye. Og hvis noe upassende ble observert, kunne man nøye seg med å sende en patrulje til det aktuelle stedet.»

Utdraget er hentet fra Humphrey Jennings *Pandæmonium 1660-1886 - The Coming of the Machine as seen by Contemporary Observers*, Papermac, London 1985:164.

DYNAMIC NETWORKS: A BRIEF REVIEW OF LITERATURE WITH LEGAL RELEVANCE

Emily M. Weitzenboeck[1]

1 Introduction

This article contains a brief literature review of the main publications in the area of dynamic networks which are of relevance to a legal study of networks (sections 2-6). To this must be added the general literature on contract law, partnership law and company law (section 7). This literature review is not meant to be exhaustive but contains the main source material for a basic legal study of the phenomenon of networks.

By networks here is meant business networks, and not other types of networks such as social media networks, or networks in public administration. The focus is on literature related to novel forms of business organisation. Many terms have been used and proposed in literature, particularly in business and management literature, to describe dynamic networks or certain aspects or variants of them. Terms like network enterprise, smart organization, virtual organizations, virtual enterprise and virtual company/corporation have been used with some of them achieving the dubious status of buzzwords for a certain period of time.

Broadly speaking, the main literature in the field may be classified under six headings (sections 2-7 below).

2 Books and articles on legal issues related to networks

Hybrids have been a recurrent research theme of Gunther Teubner who has looked at them from a socio-legal perspective in numerous essays (see, for example, Teubner, 2002, 2006, 2007 and 2009). In his 2004 book *Netzwerk als Vertragsverbund*, translated into and recently published in English (Teubner 2011), with an introduction by Hugh Collins, Teubner proposes that the German notion of connected contracts (*Vertragsverbund*) should be extended to business networks such as franchising, virtual business and just-in-time

1 This article is based on a brief literature review on business networks in chapter 1 of the author's doctoral thesis (Weitzenboeck 2010).

networks. Increased interest in contractual networks by a variety of legal scholars from different jurisdictions is also evidenced by a recent publication on networks (Amstutz and Teubner eds., 2009) following a conference on the subject held in October 2005 in Fribourg, Switzerland.

Cafaggi (ed., 2004) looks at the governance of contractual networks in Italy. This book in Italian was followed by another in 2007, edited together with Iamiceli, which also contains a compendium by other authors of various examples of business networks in Italy (Cafaggi and Iamicelli eds., 2007). Besides these two Italian books, Cafaggi has also published book chapters, working papers and articles in English on the subject.[2]

Weitzenboeck's (2010) doctoral thesis looks at the hybrid nature of networks, which have elements of both contract-based organizations and corporate forms, in particular partnership. It proposes a threefold categorisation of dynamic networks: (i) spontaneous and temporary virtual enterprises, (ii) virtual enterprises that are created for a limited time out of a pre-established pool of firms, and (iii) long-term dynamic networks with a lead partner. These different types of dynamic networks are used to examine whether and how contract and partnership law regulate and cope with such networks. There is also an empirical study of some real examples of dynamic networks from different countries.[3]

3 Monographs on legal issues of virtual enterprises

Within this group are two monographs and a doctoral thesis. Knut Werner Lange (2001) examines the legal set-up of *Virtuelle Unternehmen* under German law and follows the different stages in the life cycle of a virtual enterprise from its formation, operation up to its dissolution. Weitzenboeck (2001) has also written a monograph on *Legal issues of maritime virtual organizations* based on research in the MARVIN project[4] where, as the title suggests, the focus was on virtual organizations in the maritime domain, specifically emergency repair and routine maintenance of vessels. Cevenini's (2003) doctoral thesis on *Virtual Enterprises* first outlines five research projects funded by the European Union dealing with virtual enterprises and four examples of virtual enterprises, then attempts a definition thereof and then tries to specify a taxonomy of related legal issues. Cevenini looks at the legal identity of a

2 See, for example, Cafaggi (2005), Cafaggi (2007), Cafaggi (2008).
3 Note also Weitzenboeck (forthcoming 2012).
4 See section 4 below.

virtual enterprise and then examines some computer law issues[5] such as the electronic signature of documents, the use of cryptography, the relevance of the Electronic Commerce Directive[6] to the provision of online goods and services, and the use of electronic agents.

4 Reports of research studies funded by the European Commission

The European Commission has funded a number of projects on various aspects of virtual enterprises within its different framework programmes. This has generated various reports, conference papers and a few academic papers on this subject, few of which are of a legal nature. Of relevance to this literature review are those projects which have examined some legal issue or issues related to these entrepreneurial forms, or which have been wholly dedicated to legal issues related to dynamic networks. Within the first sub-category, that is, European Union (hereinafter abbreviated as «EU») projects in which reference to some specific legal problems related to such networks was made, one finds:

- MARVIN: (MARitime VIrtual enterprise Network 1998-2001)[7] investigated the development of an Internet-based virtual enterprise for improved ship maintenance and repair.
- VIVE: (VIrtual Vertical Enterprise – 1998-2000)[8] looked at the methodology for the setting-up and operation of a virtual enterprise, and focused on the role of an intermediary broker referred to as a «business integrator» who brings together and sets up the virtual enterprise.
- Further research on the role of the business integrator was carried out in BIDSAVER (Business Integrator Dynamic Support Agents for Virtual Enterprise – 2000-2002)[9] which, inter alia, emphasized the importance and need of a contractual framework between the participants and the business integrator.
- eLEGAL (2000-2002)[10] looked at virtual enterprises in the construction industry and its aim was «to define a framework for legal conditions and contracts regarding the use of ICT in project business».[11]

5 See further Cevenini (2003), chapter 6, pp. 179-213.
6 Directive 2000/31/EC on electronic commerce, OJ L 178, dated 17.7.2000, pp. 1–16.
7 http://research.dnv.com/marvin/summary.html (last visited 15 November 2011).
8 http://cordis.europa.eu/esprit/src/26854c1.htm (last visited 15 November 2011).
9 Information on BIDSAVER is available from http://www.ist-world.org/ (last visited 15 November 2011).
10 http://cic.vtt.fi/projects/elegal/public.html (last visited 15 November 2011).
11 See further eLEGAL website at http://cic.vtt.fi/projects/elegal/public.html (last visited 15 November 2011).

The need for a contractual framework for virtual enterprises highlighted in VIVE and BIDSAVER led the European Commission to fund a project wholly dedicated to legal issues related to virtual enterprises: ALIVE (Advanced Legal Issues in Virtual Enterprises – 2001-2003), of which the NRCCL was a project participant.[12] This project developed a taxonomy of legal issues related to virtual enterprises,[13] some of which were then examined further within the project. This included topics such as: the role of actors of the virtual enterprise, information and communications technology issues for the virtual enterprise, intellectual property issues, consumer protection issues and contracting with third parties. Within the ALIVE project, this author developed a set of legal templates meant to be the starting point for businesses to set up a legal framework for a virtual enterprise.[14]

The above projects were funded by the European Commission within its fourth (1994-1998) and fifth framework (1998-2002) programmes.

Within the thematic area of «Applied IST research addressing major societal and economic challenges» in the sixth framework programme (2002-2006), the Commission funded a number of projects under the strategic objective «networked businesses and government» with the aim of developing ICTs supporting organizational networking, process integration, and sharing of resources.[15]

Relevant projects include two large integrated projects: ECOLEAD (2004-2007)[16] and TrustCom (2004-2007).[17] An interesting research area of ECOLEAD (European COllaborative networked organizations LEADership initiative) was what they called «virtual breeding environments» which are network pools from which networked organizations can be set up.[18] ECOLEAD also developed an «agreement negotiation wizard tool» to help define the rights and obligations of the firms joining together in a virtual en-

12 Information on ALIVE is available from http://www.ist-world.org/ (last visited 15 November 2011).

13 See Van Schoubroeck *et al* (2001).

14 The three legal templates developed were the following: (i) a letter of intent, (ii) a memorandum of understanding and (iii) a virtual enterprise agreement. See further Weitzenboeck (2002a and 2002b).

15 The aim was that «[t]his shall enable networked organizations, private and public, to build faster and more effective partnerships and alliances, to re-engineer and integrate their processes, to develop value added products and services, and to share efficiently knowledge and experiences». See the references to the European Union's IST Workprogramme for 2003 and 2004 on the European Union's Cordis website at http://cordis.lu/fp6/ist.htm (last visited 15 November 2011).

16 http://ecolead.vtt.fi/ (last visited 15 November 2011).

17 For information on TrustCom, see http://cordis.europa.eu/ (last visited 15 November 2011).

18 See further on this, Weitzenboeck (forthcoming 2012, Edward Elgar).

terprise. This wizard assists (human) users to compose an agreement that represents a synthesis of the parties' commitments. The ECOLEAD project partners acknowledged that the different stages to arrive to an agreement require the intervention of human actors to make fundamental decisions and commitments. So what the project addressed was not a complex e-contracting process with a fully-automated system that generates, interprets, executes and manages a contract, but a system that could store and receive inputs into an electronic source for later interpretation by the human actor, guiding such actor through the process.[19]

TrustCom aimed «to develop a framework for trust, security and contract management within dynamic virtual organizations».[20] It carried out studies on legal risks related to access rights management and intellectual property issues related to security and contract management.

A smaller project, LegalIST (2004-2007),[21] looked at various legal issues related to information society and technologies and *inter alia* identified some examples of small and medium-sized (hereinafter referred to as «SME») clusters and highlighted some legal issues related to them.

Within this category one should also include the independent techno-legal study on virtual enterprises by Cousy *et al* (1999) that was commissioned by the European Commission and which study formed the basis of the legal taxonomy developed in the ALIVE project by the same authors.

5 Business management literature on dynamic networks

Although there is a dearth of academic legal literature on dynamic networked organizations, one finds many business management publications on the subject. The aim is not to try to mention all these publications but to highlight the more significant ones.

Two books in German on dynamic networks in Europe (in particular in the German-speaking countries) are useful in providing examples and illustrations of dynamic networks and clusters. Huber, Plüss, Schöne and Freitag's *Kooperationsnetze der Wirtschaft* (2005) contains eleven examples of various dynamic networks which are up and running (i.e. not still on the drawing board) in Germany, Austria and Switzerland. *Strategien des Handwerks* (2005) focuses on eight specialised clusters of artisans and handcraft workers

19 See Camarinha-Matos, Afsarmanesh and Ollus (eds.) (2008), p. 197.
20 See project description on http://www.ist-world.org/ (last visited 15 November 2011).
21 Information on LegalIST is available from www.ve-forum.org (last visited 15 November 2011).

in a number of countries in Europe,[22] and provides useful background material on clusters.

A much quoted book which has become a classic in this field and has helped to popularize the term «virtual corporation» is Davidow and (Michael) Malone's (1992) *The Virtual Corporation*. In 1994, the MIT Sloan School of Management undertook a five-year research initiative called «Inventing the Organizations of the 21st Century» headed by Prof. Thomas Malone which culminated in a number of highly interesting business and management oriented papers published in the book *Inventing the Organizations of the 21st Century* edited by Malone, Laubacher and Scott Morton (2003). Byrne (1993) has also written an often cited article on «The Virtual Corporation» in *Business Week* which, though not an academic publication, was one of the earliest articles that together with Davidow and Malone's book helped popularize the term «virtual corporation».

Other important non-legal academic literature on virtual enterprises include Goranson's (1999) *The Agile Virtual Enterprise* which has a business management perspective, Mowshowitz's (2002) *Virtual Organization* which has a computing angle intermixed with a sociological and organizational perspective and RAND Europe's report (2004) *Europe, Competing* on what they call «virtual, smart organizations», which report has a multi- and cross-disciplinary approach. To these must be added Castells' (2000) seminal sociological work *The Rise of the Network Society*.

6 Literature on the notion of hybrids: law and economics perspectives

Economists have long been interested in the nature of the firm, and the use of contract and the corporate form to undertake business. Coase's ground-breaking work on the nature of the firm, which was later taken up and deepened in Oliver Williamson's work on hybrids, are two basic texts. Other important economics literature on dynamic networks is the seminal article by Miles and Snow (1986) and a later article of theirs written together with Coleman (1992) where they distinguish between three types of network organizations: internal, stable and dynamic.[23] A number of papers presented at the 1995 Wallerfangen Symposium on New Institutional Economics «Transformations in the Institutional Structure of Production» and published in Volume 152 of the Journal of Institutional and Theoretical Economics also look at changes

22 Germany, Austria, Italy, France, Finland and Denmark.

23 These are discussed extensively in Weitzenboeck (2010) and forthcoming book (2012).

in the field of business organization from a law, economics and sociological perspective. Two important analytical approaches examining the changed organizational structure look at the contractual nature of the firm (Alchian and Demsetz, 1972) and refer to «three generic forms of governance – market, hybrids and hierarchy» (Williamson, 1988). Powell's paper on networks as being neither market nor hierarchy (1990) inspired response by legal scholars like Buxbaum (1993), Schanze (1991, 1993) and Teubner (2006, 2011).

7 Contract law, partnership and company law literature

Although there is a dearth of legal literature on dynamic networks, there is considerable legal literature on contract law[24] and partnership/corporate law respectively.[25]

Very insightful have been central scholarly works on legal issues related to joint ventures in some of the jurisdictions examined such as Nordtveit's (1992) classic work on Norwegian joint ventures, and Hewitt's (2008) book on joint ventures in English law, both of which also contain references to the law on joint ventures in various other jurisdictions.

8 Bibliography

Alchian, Armen A. and Harold Demsetz, (1972), «Production, information costs and economic organization», *American Economic Review*, Vol. 62, pp. 777-795.

Amstutz, Marc and Gunther Teubner (eds.), (2009). *Networks: Legal Issues of Multilateral Co-operation*, Hart Publishing, Oxford and Portland, Oregon.

Aarbakke, Magnus, (2000), *Ansvarlige Selskaper og Indre Selskaper*, 5th ed., Oslo.

Andenæs, Mads Henry, (1977), *Sameier og selskaper*, Oslo.

24 To give a few example with reference to English law, treatises on contract law include classics like those by Treitel (Peel 2007), Chitty (Beale, general ed. 2008), Cheshire, Fifoot and Furmston (Furmston 2007) and Atiyah (Smith 2005) respectively.

25 For example, to mention just a few important books on partnerships and company law, by jurisdiction – Norwegian law: Aarbakke (2000), Andenæs (1977, 2007), Normann Aarum (1994), Woxholth (2005b) and (2010), Bråthen (ed.), (1990), Gjems-Onstad (1999); English law: Farrar and Hannigan (1998), Grier (1998), Gower and Davies (2008); Italian law: Campobasso (2007), Ferri (2006), Galgano (2009); French law: Lefèbvre *et al* (2003), Merle (1998); German law: Entshaler (2007), Wendler, Tremml and Buecker (2006), and in general on German law Foster and Sule (2002).

Andenæs, Mads Henry, (2007), *Selskapsrett*, Oslo.

Beale, H.G. (gen. ed.), (2008), *Chitty on Contracts - Vol. 1: General Principles*, 30th ed., Sweet & Maxwell, London.

Bråthen, Tore (ed.), (1990), *Foretaksrett*, 2nd ed., Ad Notam Gyldendal, Oslo.

Buxbaum, Richard M., (1993,) «Is 'network' a legal concept?», *Journal of Institutional and Theoretical Economics* 149/4, pp. 698-705.

Byrne, John A., (1993), «The Virtual Corporation», *Business Week*, February 8, 1993.

Cafaggi, Fabrizio (ed.), (2004), *Reti di imprese tra regolazione e norme sociali: Nuove sfide per diritto ed economia*, il Mulino, Bologna.

Cafaggi, Fabrizio, (2005), Organizational loyalties and models of firms: Governance design and standard of duties, 6 *Theoretical Inquiries in Law*, pp. 463-526.

Cafaggi, Fabrizio and Paola Iamiceli (eds.), (2007), *Reti di imprese tra crescita e innovazione organizzativa*, il Mulino, Bologna.

Cafaggi, Fabrizio, (2007), «Fiduciary duties, models of firms, and organizational theories in the context of relational interdependencies» in Fabrizio Cafaggi, Antonio Nicita and Ugo Pagano (eds.), *Legal Orderings and Economic Institutions*, Routledge, London & New York, chapter 15, pp. 268-309.

Cafaggi, Fabrizio, (2008), «Contractual Networks and the Small Business Act: Towards European Principles?», EUI LAW Working Paper 2008/15, online at http://www.eui.eu/DepartmentsAndCentres/Law/People/Professors/CurrentProfessors/Cafaggi.aspx (last visited 19 April 2010).

Campobasso, Gian Franco, (2007), by Mario Campobasso, *Manuale di diritto Commerciale*, 4th ed., UTET, Italy.

Castells, Manuel, (2000), *The Rise of the Network Society*, Vol. I of «*The Information Age: Economy, Society and Culture*, 2nd ed., Blackwell Publishing.

Cevenini, Claudia, (2003), *Virtual Enterprises: Legal issues of the on-line collaboration between undertakings*, Seminario Giuridico dell'Università di Bologna, Giuffrè Editore, Milan.

Coase, Ronald, «The Nature of the Firm», *Economica* 4 (1937), pp. 386-405.

Cousy, Herman, Caroline Van Schoubroeck and Bart Windey, (1999), *The Virtual Enterprise – Report on Techno-Legal Issues*, Report from the Research projects No. 119519 and No. 119520, Commission of the European Communities Directorate-General XIII, Telecommunications, Information Market and Exploitation of Research, July 1999.

Davidow, William H. and Michael S. Malone, (1992), *The Virtual Corporation*, Harper Business, New York.

Davies, Paul L. (2008), *Gower and Davies' Principles of Modern Company Law*, 8th ed., Sweet and Maxwell, London.

Entshaler, Jürgen, (2007), *Gemeinschaftskommentar zum Handelsgesetzbuch mit UN-Kaufrecht*, in Jürgen Entshaler (ed.), 7th ed., Luchterhand, Germany.

Farrar, John H. and Brenda M. Hannigan, (1998), *Farrar's Company Law*, 4th ed., Butterworths, London.

Ferri, Giuseppe, (2006), by Carlo Angelici and Giovanni B. Ferri, *Manuale di diritto commerciale*, 12th ed., UTET, Italy.

Foster, Nigel and Satish Sule, (2002), *German legal system and laws*, 3rd ed., Oxford University Press, Oxford.

Furmston, Michael, (2007), *Cheshire, Fifoot & Furmston's Law of Contract*, 15th. ed., Oxford University Press, Great Britain.

Galgano, Francesco, (2009), *Diritto commerciale: Le società. Contratto di società. Società di persone. Società di azioni. Altre società di capitali. Società cooperative.* Zanichelli, Bologna.

Goranson, H.T., (1999), *The agile virtual enterprise: Cases, metrics, tools*, Quorum Books, Connecticut, U.S.

Gjems-Onstad, Ole, (1999), *Valg av Selskapsform*, 4. utgave, Ad notam Gyldendal, Oslo.

Grier, Nicholas, (1998), *UK Company Law*, Wiley, London.

Hewitt, Ian, (2008), *Joint Ventures*, 4th ed., Thomson, Sweet & Maxwell, U.K.

Huber, Charles, Adrian Plüss, Roland Schöne and Matthias Freitag (eds.), *Kooperationsnetze der Wirtschaft: Einführung, Bausteine, Fallbeispiele*, vdf Hochschulverlag AG and der ETH Zürich.

Landschaft des Wissens (2005), *Strategien des Handwerks: Sieben Portraits außergewöhnlicher Projekte in Europa,* Haupt Verlag AG, Berne-Stuttgart-Vienna.

Lange, Knut Werner (2001), *Virtuelle Unternehmen: neue Unternehmenskoordination in Recht und Praxis*, Verlag Recht und Wirtschaft GmbH, Heidelberg.

Lefèbvre, Dominique, Edwige Mollaret-Laforêt, Christian Guiter and Charles Robbez Masson, (2003), *Droit et enterprise: Aspects juridiques, sociaux, fiscaux*, 9th ed., Presses Universitaires de Grenoble, France.

Malone, Thomas W., Robert Laubacher and Michael S. Scott Morton, (eds) (2003), *Inventing the Organizations of the 21st Century*, MIT Press, Cambridge, Massachusetts.

Merles, Philippe, (1998), *Droit commercial: Sociétés commerciales*, 6th ed, Dalloz, France.

Miles, Raymond E. and Charles C. Snow, (1986), «Organizations: New concepts for new forms», *California Management Review*, Vol. 28, No. 3, (1986) reprinted in Peter J. Buckley and Jonathan Michie (eds.), *Firms, Organizations and Contracts*, OUP, Oxford, 1996, pp. 429-441.

Mowshowitz, Abbe (2002), *Virtual Organization: Towards a theory of societal transformation stimulated by information technology*, Quorum Books, Connecticut, US & London, England.

Nordtveit, Ernst, (1992), *Oppdragssamarbeid – Joint Ventures: Samarbeidsformer innenfor entreprenørverksemd, konsulenttenester og leverandørindustri*, Alma Mater Forlag AS, Bergen.

Normann Aarum, Kristin, (1994), *Styremedlemmers erstatningsansvar i aksjeselskaper*, Ad Notam Gyldendal, Oslo.

Peel, Edwin, (2007), *Treitel: The Law of Contract*, 12th ed., Sweet & Maxwell, London.

Powell, Walter W. (1990), «Neither Market nor Hierarchy: Network forms of organization», *Research in Organizational Behaviour*, Vol. 12, pp. 295-336.

Rand Europe (2004), *Europe, Competing: Market Prospects, Business Needs and Technological Trends for Virtual, Smart Organizations in Europe*, February 2004, Rand Europe.

Schanze, Erich, (1991), «Symbiotic contracts: Exploring long-term agency structures between contract and corporation», in Joerges, Christian, (ed.), *Franchising and the Law: Theoritical and Comparative Approaches in Europe and the United States*, Nomos Verlagsgesellschaft, Baden-Baden, Germany.

Schanze, Erich, (1993) (ed.), «Symbiotic Arrangements», *Journal of Institutional and Theoretical Economics*, Vol. 149, pp. 691-697

Smith, Stephen A. (2005), *Atiyah's Introduction to the law of contract*, 6th ed., Clarendon Press, Oxford.

Snow, Charles C., Raymond E. Miles, Henry J. Coleman Jr., (1992), «Managing 21st Century Network Organizations» in *Organizational Dynamics*, Winter pp. 5-20.

Teubner, Gunther (2002), «Hybrid Laws: Constitutionalizing Private Governance Networks», in Robert Kagan and Kenneth Winston (eds.), *Legality and Community: On the Intellectual Legacy of Philip Selznick*, Berkeley Public Policy Press, Berkeley 2002, pp. 311-331.

Teubner, Gunther, (2006), «Coincidentia oppositorum: Hybrid Networks Beyond Contract and Organization», Storrs Lectures 2003/04 Yale Law School, in Robert Gordon and Mort Horwitz (eds.), *Festschrift in Honour of Lawrence Friedman*, Stanford University Press, available online at http://ssrn.com/abstract=876939 (last visited 19 April 2010).

Teubner, Gunther, (2007), «In the Blind Spot: The Hybridization of Contract», in *Theoretical Inquiries in Law* 8, 2007, 51-71.

Teubner, Gunther (2009), "'And if I by Beelzebub cast out Devils,...': An Essay on the Diabolics of Network Failure", in *German Law Journal* 10, Special Issue: The Law of the Network Society: A Tribute to Karl-Heinz Ladeur, pp. 115-136.

Teubner, Gunther, (2011), *Networks as Connected Contracts*, translated by Michelle Everson, edited with an Introduction by Hugh Collins, Hart Publishing, Oxford and Portland, Oregon. This is a translation of *Netzwerk als Vertragsverbund: Virtuelle Unternehmen, Franchising, Just in Time in sozialwissenschaftlicher und juristischer Sicht,* (2004), Nomos, Baden-Baden.

Weitzenboeck, Emily M. (2001), *Legal issues of maritime virtual organizations*, Complex 4/2001, Unipub Forlag.

Weitzenboeck, Emily M., (2002a) *VE Model Contracts*, ALIVE project deliverable D17a, dated 27/11/2002.

Weitzenboeck, Emily M., (2002b) *The VE Interchange Agreement*, ALIVE project deliverable D17, dated 27/11/2002.

Weitzenboeck, Emily M., (2010), *Between contract and partnership: Dynamic networks as collaborative contracts and more*, Dissertation for the degree of PhD 2010, Faculty of Law, University of Oslo, Oslo.

Weitzenboeck, Emily M., (forthcoming 2012), *A Legal Framework for Emerging Business Models: Dynamic Networks as Collaborative Contracts*, Edward Elgar Publishers.

Wendler, Michael, Bernd Tremml and Bernard Buecker (eds.), (2006), *Key Aspects of German Business Law*, 3rd ed, Springer, Germany.

Williamson, Oliver, E. (1988), «The Logic of Economic Organization», *Journal of Law, Economics and Organizations*, 4, pp. 65-93.

Woxholth, Geir, (2005b), *Selskapsloven: Kommentarutgave*, 5th ed., Ad Notam Gyldendal, Oslo.

Woxholth, Geir, (2010), *Selskapsrett*, 3rd ed., Gyldendal Akademisk, Oslo.

GOVERNANCE MODELS FOR INTEROPERABLE eIDs

Tobias Mahler[1]

Abstract

Current implementations of electronic identity in Europe are rather diverse; they include state-driven identity management frameworks as well as private sector frameworks and different forms of public-private collaborations. This diversity may represent a major challenge for the deployment of information society services addressed towards the European internal market. This raises the question: How can we achieve interoperability of electronic identities across Europe, and potentially beyond Europe's borders? This paper argues that the interoperability of electronic identity could be governed by a multi-stakeholder governance framework that brings together different parties with interests in the provision and use of electronic identities. Such a governance framework could, for example, consist in designing and operating a portal with common functionalities that allows interoperable authentication across multiple domains and contexts. Inspiration for the governance of such a portal could come both from existing successful implementations of electronic identity and from multi-stakeholder institutions that have proven useful in Internet governance.

Key words

Electronic identity; Internet governance; Competition; Europe

1 Norwegian Research Center for Computers and Law (NRCCL), the Faculty of Law, University of Oslo, tobias.mahler@jus.uio.no. Thanks are due to the European Commission's Joint Research Centre, Institute for Prospective Technological Studies (IPTS), for the invitation to present this paper at the workshop «Electronic Identity for Europe» in Cyprus. This paper has been submitted for publication to the Journal of International Commercial Law and Technology. Thanks go also to Lee Bygrave, Emily Weitzenboeck, and Kevin McGillivray, who have provided valuable comments to an earlier draft, and to Robert Queck for discussing with me the status of identity services in the electronic communications framework. However, any errors or omissions are entirely mine.

Introduction

Interoperable electronic identity (eID) is often considered a necessary ingredient of cross-border interactions and transactions over the Internet. Anyone building a framework for interoperable eIDs needs to address a wide array of issues, including the choice of a technical framework, the context for which eIDs shall be used (e.g., eGovernment, eBusiness, or both) and the selection or development of a suitable legal framework. Many of these issues are, in practice, dependent on and intertwined with the institutional arrangements put in place to govern the eID framework. For example, amongst the interesting legal issues is the liability of actors involved in the provision and use of eIDs.[2] The liability of parties to an eID framework depends evidently, in part, on the roles of the collaborators and their legal status. Similarly, the provision and use of eIDs needs to comply with legal requirements—for example, under data protection law—and ensuring compliance may have to be organised across a network of collaborating parties.

Identity management[3] systems are currently implemented in a variety of governance structures and models in Europe. These span from primarily state-driven eIDs to different degrees of public-private collaborations and private sector solutions. The private sector's involvement is not necessarily surprising, because both private and public entities might, in principle, play a role in the provision and use of eIDs. Besides, the key role of the private sector in eID innovation is beyond question. While the variety of implementations and governance models in Europe may be seen as a challenge for interoperability, it could also be viewed as an illustration of some of the breadth of available options and solutions for the future governance of eID in Europe and beyond. This paper discusses a few basic models for the governance of eID and exemplifies these based on selected examples of existing European eID implementations.

The structure of this paper is as follows: Section 1 introduces the concept of eID and the roles involved in issuing and using interoperable eIDs. This paper focuses primarily on interoperable eID in a European context. Therefore, Section 2 provides a very brief outline of the European legal framework for eID. However, the main interest of this paper does not centre on the legal is-

2 See, e.g., Georg Borges, „Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis: Ein Gutachten für das Bundesministerium des Innern," (2010). Regarding liability issues in the context of digital certificates see, e.g., Rolf Riisnæs, *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar: en tillitsorientert tilnærming til sertifikatutstederens villedningsansvar* (Bergen: Fagbokforlaget, 2007).

3 For an introduction to identity management see Roger Clarke, «Identity Management,» (Xamax Consultancy, 2004).

sues as such, but on the governance of interoperable eIDs. Therefore, Section 3 introduces the concept of governance; Section 4 discusses the governance of other identifiers—such as domain names, and Section 5 explains how interoperable eID can be framed as a governance challenge. The paper then turns towards the core of eID governance. In this context we can make a rough distinction between eID provision and use. The subsequent Sections (6, 7 and 8) focus on eID provision and describe three basic models of eID provision, respectively based on public, private and public-private governance structures. When eIDs are offered based on very dissimilar governance structures, this may result in a rather heterogeneous picture, which may be challenging in terms of interoperability. Therefore, Section 9 focuses on the governance of interoperability itself. One solution to the problems of inconsistent and diverging eIDs may be to create an intermediary agency (an authentication authority) that is able to handle interoperability problems directly. This approach, as well as its governance challenges, is explained based on a concrete example of an eID portal. The concluding Section 10 argues that the latter model could potentially be employed to address eID interoperability not only at the European level, but also in a wider context.

1 eID and interoperability

The need for eID arises in part from the fact that the Internet is designed to be somewhat agnostic to the identity of its users. Domain names and IP numbers are machine identifiers, rather than identifiers of persons, even though personal identification may be possible.[4] Therefore, we use identifiers such as e-mail addresses or user names to identify a person. An eID can be the basis for different functions, in particular authentication and signature.[5] We are here particularly interested in eIDs that can be used for authentication purposes. A relying party can *authenticate* a claimed identity by examining one or more authenticators (such as passwords or other credentials) to verify the legitimate

4 See, e.g., P. Lundevall-Unger and T. Tranvik, «IP Addresses–Just a Number?,» *International Journal of Law and Information Technology* 19, no. 1 (2011). Moreover, it may be possible to use a URL as an identifier of an eID, as foreseen in the W3C specification «WebID 1.0: Web Identification and Discovery», W3C Editor's Draft, 17 October 2011, available at http://www.w3.org/2005/Incubator/webid/spec/ (last visited 10 November 2011).

5 Regarding electronic signatures, see Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p. 12 (e-Signatures Directive).

use of an identifier (e.g., a user name).[6] Different eIDs may vary in their level of assurance, depending on certain security aspects of the authenticator(s).

The notion of eID is here not used as a precisely defined technical concept; the IT literature usually applies a more specific taxonomy.[7] However, it can be based on the technical notion of «identity» in the sense of «any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons».[8] The use of eIDs in identity management systems can be distinguished from directory services that provide some information connected to an identifier. Directory services are not designed to facilitate either authentication or signature. An example of a directory service is the WHOIS service, which provides information about the technical and administrative points of contact administering domain names.[9] Mueller and Chango have described the WHOIS service as a «surrogate identity system:» [10] The data in the WHOIS record is as close as the Internet gets to an identity card.[11] The WHOIS service is not aimed at authentication, even though it may play a central role for the creation of trust on the Internet, particularly when combined with adequate security mechanisms.[12]

Despite this potential similarity in function, the primary focus of this paper is not on directory services, but on eIDs.[13] At the same time, we cannot delve into the details of eID technologies, because the centre of attention is on the governance of eIDs. We are particularly interested in eIDs that allow an identity holder to use an interoperable eID in an identity management framework spanning across multiple contexts, such as those of eBusiness and eGovernment. This use and re-use of eIDs within different contexts requires

6 Clarke, «Identity Management,» 3. Authentication is closely related to, but needs to be distinguished from, *authorization*, i.e., the decision about an authenticated user's privileges.

7 A. Pfitzmann and M. Hansen, «A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,» (version v0.34, 2010).

8 See ibid., 30.

9 Cf., e.g., Article 16 (1) of Regulation (EC) No. 874/2004. See further D.I. Cojocarasu, «Legal Issues Regarding WHOIS Databases,» (Oslo: Senter for rettsinformatikk, 2009).

10 Milton Mueller and Mawaki Chango, «Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy,» *Journal of Information Technology & Politics* 5, no. 3 (2008): 304.

11 Ibid., 310.

12 An example of such security mechanisms are Domain Name System Security Extensions (DNSSEC), based on specifications for securing certain kinds of information provided by the Domain Name System. See, e.g., https://www.iana.org/dnssec/.

13 However, such directory services can be a useful basis for comparing governance models, as shown below in Section 4.

some degree of interoperability, both in the sense of technical standardisation[14] and in terms of organisational collaboration.[15] Strongly simplified, technical interoperability implies, for example, that an eID issued by one actor (e.g., the identity provider) can be understood and used by another actor (e.g., a relying party). This is usually embedded in some kind of identity management framework, which may require quite complex organizational collaboration. For example, the issuing of an eID may involve collaboration between a registration authority (enrolling the eID holder), an identity provider (who may issue the eID itself, or on whose behalf the eID is issued) and an agency that distributes the eID (for example, on a smart card). Similarly, the use of an eID could involve not only relying parties, but also authentication authorities[16] and perhaps even further intermediaries and service providers.

The governance framework has to address both the provision and the use of interoperable eIDs:[17] First, one needs to ensure that eIDs are created and issued through a collaboration of registration authorities, identity providers, and possible distributors. This corresponds to the eID *registration phase*. Second, there are governance issues related to the use of eIDs during the *authentication phase*. Interoperability is of particular importance for the latter phase. There may be many ways to ensure interoperability, but this paper will focus on institutional solutions involving an intermediary, in particular an authentication authority (see Section 9).

2 The European legal framework for eID

Any framework for eID has to be related to, and comply with, the applicable legal framework. This section will briefly note a few European legal instruments that may be at least partly relevant to the provision and use of interoperable eIDs. In principle, interoperability of eIDs is not only a European issue; it can indeed be seen as a global challenge. Nevertheless, within the European discourse about eID it may be prudent to focus on a European solution initially, because an interoperable eID in Europe would be a particularly useful facilitator for the European internal market and for eGovernment in Europe. Indeed,

14 See generally on interoperability Laura DeNardis, *Opening standards: the global politics of interoperability*, The information society series (Cambridge, Mass.: MIT Press, 2011).

15 See, e.g., Thomas Olsen and Tobias Mahler, «Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust',» *Computer Law & Security Report* 23, no. 4+5 (2007).

16 On authentication providers see R. Leenes et al., «D.2.2 — Report on Legal Interoperability,» (Stork eID Consortium, 2009), 23-27.

17 Ibid., 24-25.

interoperability of eIDs has been identified as a key challenge for eGovernment and for some aspects of eBusiness in Europe.[18] One of the elements in that discussion is whether Europe currently lacks an adequate regulatory framework for eID.[19] What may be called «the legal framework» consists of a patchwork of partly relevant rules in several legal instruments, including at least the EU electronic signature directive[20] and the data protection directives.[21] Thus, all identity management systems must comply with the applicable data protection laws.[22] In complex identity management systems consisting of several collaborating parties, this requires a number of potentially difficult assessments, such as who is acting as a data *controller* and who is a data *processor*.[23] For example, in a series of cases before the Norwegian Data Protection Agency, the latter body questioned a number of operational details in a Norwegian eID

18 N. N. G. de Andrade, «Towards a European eID regulatory framework. The Legal Gaps, Barriers and Challenges of Constructing a Legal Framework for the Protection and Management of Electronic Identities,» in *European Data Protection: In Good Health?*, ed. S. Gutwirth, et al. (Springer, 2012 - forthcoming).

19 The lack of «an appropriate regulation regarding eID on a European level» was ascertained by T. Myhr, «Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution:: or I am 621216-1318, but I am also 161262-43774.1 Do you know who I am?,» *Information Security Technical Report* 13, no. 2 (2008): 77. Concurring with this view de Andrade, «Towards a European eID regulatory framework. The Legal Gaps, Barriers and Challenges of Constructing a Legal Framework for the Protection and Management of Electronic Identities,» Section I.4.5.

20 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p. 12 (e-Signatures Directive).

21 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), L 281 , 23/11/1995, p. 0031 – 0050; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002-07-31, L 201, pp. 37 – 47, as amended.

22 See further Olsen and Mahler, «Identity Management and Data Protection Law: Risk, Responsibility and Compliance in 'Circles of Trust'.»; Thomas Olsen, «Personvernøkende identitetsforvaltning» (University of Oslo, 2010).

23 According to the Data Protection Directive 95/46/EC (above, note21), Article 2 (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law. According to Article 2 (e) of the same Directive, 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

system utilized in the eGovernment context.[24] The agency's criticism related not only to insufficiently clarified roles of participants, but also to whether there existed sufficient legal basis for all aspects of the processing of personal data. It is beyond the scope of this paper to discuss these issues in any detail.

However, it may be in order to highlight one minor aspect of the legal framework that is usually omitted from legal discussions about eIDs—perhaps for a good reason. This relates to the fact that the EU regulatory framework for electronic communications was in 2009 extended with explicit rules about «identity services» related to electronic communications. These rules may not be directly applicable to eIDs used for eBusiness or eGovernment services (as shown below), because the rules focus on the underlying communications network, rather than on the services. However, these rules are nevertheless of interest here, if only to illustrate the possibility of focusing on competition in the eID context. Readers without specific interest in the EU legal framework may consider skipping the remainder of this section and continuing directly with Section 3 below.

In order to understand «identity services» related to electronic communications, we need to briefly outline their legal context. In 2009, the «Better Regulation» Directive[25] introduced the notion of «associated services» into the electronic communications Framework Directive.[26] According to Article 2 (ea) of the amended Framework Directive, associated services include, *inter alia*, «*identity*, location and presence service» (emphasis added). Identity services are not defined in the Directive or elsewhere in the electronic communications framework, but «identity» is in the electronic communications context sometimes used in the context of caller identification, which is perhaps closest to a directory service as described above. In general, the concept of «associated services» is relevant because it triggers the authority and obligation of national regulatory authorities to promote competition in the provision of electronic

24 The Norwegian Data Protection Agency (Datatilsynet), control reports 08/00291and 08/00297; decisions «Altinn sentralforvaltning» (2008) and «Skattedirektoratet og Altinn (2008). For an overview of these cases see Olsen, «Personvernøkende identitetsforvaltning,» 165 et seq.

25 Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337/37.

26 Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, OJ L 108 of 24.4.2002.

communications services and associated services.[27] Moreover, pursuant to the Access Directive, operators with significant market power may be required to provide access to associated services, including identity services.[28]

However, despite the initial similarity of terminology, it is not certain that these rules will apply to the typical eID services used in eGovernment and eBusiness, because these would typically qualify as so-called information society services.[29] This is important because, in order to qualify as an associated service under the Framework Directive, the service has to be associated with an *electronic communications service*—i.e., it needs to be related to the conveyance of signals on electronic communications networks, which explicitly excludes information society services such as eBusiness and eGovernment.[30] Thus, the provisions on «identity services» in the electronic communications context would probably not be directly applicable to the context of eIDs in eBusiness and eGovernment. eIDs are usually offered by actors involved in either eBusiness or eGovernment, with no particular role in the conveyance of signals on electronic communications networks. It remains to be seen how these rules will be applied to identity management systems operated by, e.g., telecoms operators.

However, these rules can serve here at least to illustrate the competition aspect of eIDs. Competition in a market for eIDs is indeed one of the relevant governance issues related to interoperable eIDs.

3 Governance

The problems of interoperability and competition in the eID context are here portrayed as governance challenges. The aim of this section is to briefly introduce the concept of governance, particularly in an Internet context.

27 See Article 8 (2) of Directive 2002/21/EC (note 26 above). In any case, a NRA has in practice to balance several aims, including, for example, consumer protection and competition. Thus, this provision may not in itself be sufficient to require NRAs to prioritize competition.

28 See Article 12 (1) (j) Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), as amended by Directive 2009/140/EC (note 25 above).

29 Information society services are defined as «any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services» in Article 1 of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998, laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, OJ L 24, 21.7.1998, p. 37.

30 See Article 2 (c) of Directive 2002/21/EC (note 26 above).

Governance can be defined as a process of steering.[31] Its etymological origins include the ancient Greek word *kybernan* and the Latin *gubernare*, 'to steer' as well as *kybernetes*, «pilot» or «helmsman.» Thus, the double nature of both (i) the act of governing and (ii) the role of a governor are relevant to understand the concept. However, while governance may involve an authority relationship, this is not necessary by definition. Governance can take many forms, it can be carried out alone or collaboratively, top-down or bottom-up, and may exists across levels of social organization, e.g. at intra-organizational, national, European or global levels.

Of particular relevance for the eID context is Internet Governance. This can be defined based on the following working definition, drafted by the UN-appointed Working Group on Internet Governance and included in the Tunis Agenda adopted by the World Summit on Information Society:

> *«Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.»*[32]

Central for this definition is the focus on the role of multiple stakeholders, including governments, the private sector and civil society. This multi-stakeholder focus is of particular relevance to the Internet, which has historically evolved with very limited involvement by states. While the discussion about multi-stakeholderism is still continuing in international fora, many of the key elements of the Internet are at the time of writing governed by an institutional ecosystem that facilitates a high degree of influence for different stakeholders.[33] For the purposes of the present paper, it is particularly interesting to note that Internet governance focuses, inter alia, on governing identifiers.

---

31 This definition, its historical origins and connotations are based on William J. Drake, «Introduction: The Distributed Architecture of Network Global Governance,» in *Governing global electronic networks: International perspectives on policy and power*, ed. William J. Drake and Ernest J. Wilson (Cambridge, Mass.: MIT Press, 2008), 7 et seq.ed. William J. Drake and Ernest J. Wilson (Cambridge, Mass.: MIT Press, 2008

32 Tunis Agenda for the Information Society, World Summit on the Information Society, 18 November 2005, paragraph 34.

33 See, e.g., Lee A. Bygrave and Jon Bing, *Internet Governance: Infrastructure and Institutions* (Oxford: Oxford University Press, 2009).

4 Governance mechanisms for identifiers

Amongst the basic functions of an eID is to identify a person. This identification function is interesting when we compare it to other identifiers, such as domain names and telephone numbers. My conjecture is that the spectrum of governance models in use for other identifiers might illustrate some of the available policy choices when designing an eID framework. Before we address the specific problems related to eID, we should therefore take a brief look at governance mechanisms used for other interoperable identifiers.

The governance of domain name addresses and IP (Internet Protocol) numbers is amongst the key issues in global Internet governance. Both of these identifiers are governed by a dedicated institutional framework that is administrated primarily by the Internet Corporation for Assigned Names and Numbers (ICANN) and its supporting organizations.[34] The most striking characteristic of this institutional framework is the substantial private sector influence, which is built into ICANN's decision-making procedures. At the same time, the ICANN model illustrates the difficulties with agreeing on a global framework for identity-related services, i.e., the contact information available in the WHOIS directory service. At the time of writing ICANN is still struggling with a reform of the WHOIS system that adequately addresses issues such as data protection and law enforcement.[35]

In addition, there are other identifiers of international relevance, such as radio frequency identification (RFID) tags which are administered by the private sector[36] and telephone numbers which are administered in part at national level—with substantial involvement of both national regulatory agencies and telecom operators—and in part at the international level under the auspices of the International Telecommunications Union—also with significant industry participation.

In summary, the governance of other interoperable identifiers is carried out in a number of different institutional models. While many identifiers are

34 See, e.g., A.M. Froomkin, «Habermas@discourse.net: Toward a critical theory of cyberspace,» *Harvard Law Review* 116, no. 3 (2003); Milton Mueller, *Ruling the root: Internet governance and the taming of cyberspace* (Cambridge, Mass.: MIT Press, 2002).

35 See http://gnso.icann.org/issues/whois/policies. For the historical background see Mueller and Chango, «Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy.»

36 See further http://www.gs1.org/epcglobal (last visited 20 September 2011). The discussion of RFID governance falls outside the scope of this paper. For a multi-stakeholder governance model for RFID see http://www.rfid-in-action.eu/public/results/rfid-stakeholder-model (last visited 20 September 2011). The latter was created to achieve a structured model of all stakeholder groups that are relevant for the development, deployment and operation of RFID systems.

governed by stakeholders from the private sector alone (e.g. RFIDs), other governance models involve some degree of collaboration between stakeholders. In some cases, such as telephone numbers, this involves collaboration between stakeholders from the private sector with governmental authorities. Such public-private cooperation may not be sufficient to justify the label «multi-stakeholder governance», but there are also examples of the latter, where additional stakeholders such as end-users and civil society have some measure of influence. My argument in this paper is that some of these governance models could be usefully applied to govern the development and use of interoperable eIDs. We might learn from successful governance models developed in other contexts and apply the lessons learned there to address some of the challenges with eID interoperability.

5 Interoperable eID as a governance challenge

If the interoperability of eIDs is recast as a governance challenge, it can be analysed in terms of the influence exercised by different stakeholders. A multi-stakeholder governance framework for eIDs would require that we first identify relevant stakeholders.

Who are the stakeholders related to the issuing and use of an interoperable eID? The answer to this question may depend to some degree on the specific context, so this must here be addressed in the abstract. The starting point can be the above-mentioned roles typically related to an eID, i.e., identity holders, registration authorities, identity providers, authentication authorities, relying parties, and other possible intermediaries and service providers.[37] Of particular interest are the roles of identity providers, registration authorities and authorization authorities, because these actors arguably have the greatest influence on the governance of an eID framework. At the same time, relying parties and identity holders should not be forgotten, as these two stakeholder groups are the primary «users» of eID. Moreover, a governance model should also include intermediaries with a core focus on interoperability, who might be able to address and manage some of the existing inconsistencies between different eID implementations (see further Section 9).

Any of these roles can, in theory, be filled by a person from the public or private sector. Moreover, also end-users and civil society hold stakes in an eID system, and their interests should be represented in a full multi-stakeholder framework. However, in order to limit the scope of this paper, we shall here concentrate primarily on the roles of business and the public sector.

37 See Section 1.

We may roughly distinguish three very basic models of eID governance, namely:

- public eID governance,
- private eID governance, and
- governance by public-private partnerships.

Each sector brings with it the typical governance mechanisms. This is particularly evident when we focus on governance through legally binding rules. While private sector governance is limited to contractual governance, the public sector may in addition also employ legislative rule-making. Where the public and the private sectors collaborate on an equal footing, this usually implies some element of contractual governance. Of course, regardless of the specific governance model, any eID framework will obviously need to be operated within the context of the applicable laws. Thus, issues such as compliance with data protection law arise regardless of the chosen eID governance model.

As mentioned above,[38] we may distinguish between the governance of eID provision (the registration phase) and the governance of eID use (authentication phase), during which interoperability is essential. Any of the above three models could theoretically be applied to governance issues of both phases, as illustrated in Table 1.

Table 1: eID provision and use within the three governance models

eID provision and use:	Public	**Private**	**Public-private**
eID provision (registration phase)	Section 6	Section 7	Section 8
eID use (authentication phase)	Section 9		

The following sections (6-8) present and exemplify the three above mentioned governance models based on selected aspects of eID provision in several European countries. These sections focus primarily on the institutional framework in place to govern the issuance of eIDs. Thereafter, Section 9 is dedicated to the governance of the authentication phase, with a particular focus on how interoperability of eIDs can be facilitated.

38 See Section 1.

6 Public eID provision

The ideal type[39] of public eID provision is a setting in which an eID is issued and administered by organs of a state. The classical example of this model is the role of a state issuing a passport or a citizen card. In this case, a public authority functions as a registration authority and the organ issuing the passport is the «identity provider». This model can, to some extent, be transposed into the Internet context.

The German eID framework serves here as an example of an eID provided and governed by the public sector. In Germany, an eID can be included in the citizen card, which is at the same time an identification document in the off-line context.[40] Thus, one of the eID's functions is to resemble the identification in the off-line world, traditionally based on official documents such as passports. Just like the latter, the German eID could in principle be used both in a governmental context and for all other contexts where identification is needed. However, while anyone can read the physical ID card, not everyone can access the eID stored on it. Relying parties in eBusiness or eGovernment need a specific certificate, called an access certificate, to access the eID on the card. The access certificate also specifies what kinds of information may be communicated, such as the identity holder's address or age. This eID framework does not seem to include any authentication authorities, as the authentication is either directly carried out by the relying party or outsourced to other parties.[41]

The German eID governance framework is primarily of a public sector nature. The use of these eID is governed by the German act on personal identification cards and electronic identification.[42] The card itself is issued by the authorities and produced by the Federal Printing Office «Bundesdruckerei».

It is not apparent that other stakeholders, such as the private sector or end-users, are directly participating in the governance of this eID. However, it is noteworthy that the German constitution was recently amended to introduce a collaborative framework involving both the federal government and the respective state governments (Länder) in the context of IT systems.[43] This was the basis for establishing an IT planning council, which also includes re-

39 An ideal type is an analytical construct that can be used to highlight specific features of real cases.

40 See, e.g., G. Hornung and A. Roßnagel, «An ID card for the Internet-The new German ID card with 'electronic proof of identity',» *Computer Law & Security Review* 26, no. 2 (2010).

41 See also Leenes et al., «D.2.2 — Report on Legal Interoperability,» 81 et seq. On authentication authorities see further below, Section 9.

42 Gesetz über Personalausweise und den elektronischen Identitätsnachweis, 18.06.2009.

43 See Article 91c of the German Constitution (Grundgesetz).

presentation from municipalities and the data protection authorities.[44] Thus, there is collaboration between several stakeholders, but only from the public sector. While civil society and business interests are not formally represented, it follows from the strategy of the IT council that the involvement of these stakeholders should be increased.[45] This could become relevant when the IT council will develop an eID strategy in the near future.[46]

7 Private eID provision

There are many examples of eIDs that are issued by the private sector. At the time of writing many companies rely on user-names and passwords that can only be used for internal purposes. Yet there is an increasing use of interoperable private-sector eIDs, such as the option to authenticate a user based on credentials used in social networks like Facebook.[47] The fact that Facebook at the same time relies on eIDs issued under the open standard OpenID[48] illustrates that interoperability of private sector eIDs may go both ways. In other words, the identity provider for one eID may at the same time be a relying party accepting another eID, and both eIDs could be used interchangeably to authenticate users for certain contexts. Of particular interest for the present paper is the possibility to use such private sector eIDs in an eGovernment context.[49]

In addition, in some European countries there is also a market for interoperable private-sector eIDs that offer a high level of security. Such eIDs can be offered, for example, on a smart card, and they may fulfil the security requirements for eGovernment in some countries. Such use raises, of course, specific

44 For a general overview of the IT Planning Council see www.it-planungsrat.de (last visited 10 November 2011).

45 National E-Government Strategy, IT Planning Council decision of 24 September 2010, goal 12, page 12. The strategy is available from the Council's website http://www.it-planungsrat.de (last visited 10 November 2011).

46 IT Planning Council, decision 2011/18. Interestingly the planning council notes explicitly that the eID strategy should involve the authorities at federal, state and municipal level, but makes no mention of civil society or business users of eID.

47 See Omer Tene, «Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services» in this issue.

48 See Luke Shepard, «Facebook Supports OpenID for Automatic Login», Developer Blog, May 18, 2009, http://developers.facebook.com/blog/post/246/. OpenID is is a Web registration and single sign-on protocol that lets users register and login to OpenID-enabled websites using their own choice of OpenID identifier. It is offered by the OpenID Foundation, an international non-profit organization. See further www.openid.net.

49 D. Thibeau and R. Drummond, «Open trust frameworks for open government: Enabling citizen involvement through open identity technologies,» in *White paper, OpenID Foudation and Information Card Foudation* (2009).

governance issues related to the authentication phase, which will be further addressed below in Section 9.

8 Public-private eID provision

The third basic type of eID provision is based on different types of public-private partnerships. This approach was chosen for the provision of eIDs in several European countries, including Denmark and Austria. The Danish eID is offered by a public-private partnership based on consortium agreement amongst the collaborating parties and a contract with the end-user.[50]

By comparison, the Austrian eID is based on the Austrian eID act and is provided with significant involvement of the Austrian government as well as the private sector. The details of this collaboration cannot be exhaustively presented here, but a brief and simplified summary may illustrate the essentials.[51] It is perhaps best to describe this collaboration by following the life-cycle of an eID. This starts with the registration phase, where a «certification service provider» is responsible for verifying the citizen's identity as part of the registration procedure. This entity also as requests a digital signature called an «identity link» from the register authority (public sector). While the identity provider is lastly the Austrian register authority, the issuers of the «Citizen Card» can be both private and public parties. Interestingly, the identity provider is consulted only during the issuance of the Citizen Card. During use of a Citizen Card, no identity provider is consulted, because only the identity link is used.

9 Governance of eID interoperability

So far we have focused primarily on the issuance of interoperable eIDs. We should now turn our attention to the governance of eID interoperability itself. The starting point for this is a situation where there is a multiplicity of available eIDs, as well as many potential relying parties. An example is the variety of eIDs currently available in Europe, which potentially could be used in eBusiness and eGovernment across Europe, but which currently cannot be used due

50 This eID solution is called «NemID» and its governance by the Danish banking sector and the National IT and Telecom Agency is briefly mentioned in English at https://www.nemid.nu/om_nemid/about_nemid/ and further explained in Danish at https://www.nemid.nu/om_nemid/hvad_er_nemid/parterne_bag_nemid/ (both last visited 10. November 2011). The organizational framework may change in the near future, because the agency will be discontinued by the recently elected Danish government.

51 For a more detailed account of the Austrian eID framework see Leenes et al., «D.2.2 — Report on Legal Interoperability,» 49 et seq.

to lacking interoperability. This lack of interoperability can have technical, organizational and legal dimensions, and it may to some degree be influenced by relying parties' insufficient knowledge about existing eIDs and lack of trust for ID providers and other parties involved in issuing an eID. This raises the question whether it would be possible to design governance structures that could facilitate the interoperability of otherwise incompatible eIDs. Would it be possible to design a governance framework that could define policies for eID interoperability, perhaps even within a multi-stakeholder framework? Experiences with governance structures for other identifiers as well as existing models for eID interoperability indicate, in my view, that we should not necessarily disregard this possibility.

The basic structure of such a governance framework would imply that an intermediary entity—an authentication authority—facilitates interoperability between different eID providers on the one hand and relying parties on the other hand. This possibility will here be exemplified with the Norwegian eID portal («ID-porten»). Within the Norwegian eGovernment context, this portal is a key enabler for interoperability of eIDs from the private and the public sectors. This is to say that a range of governmental service providers (i.e., relying parties) can use the ID portal to authenticate[52] their users, who may choose among several available eIDs issued by private-sector and public-sector entities.

In the following I will briefly introduce the portal model as it may be experienced from the perspective of an end-user. This description will omit most of the technical details that are necessary to make the model work and will rather focus on the overall structure and the underlying governance model. A user who wishes to authenticate herself to a governmental service provider (for example, the tax authorities) participating in this scheme may pick one of several pre-selected eIDs. In practice, all inhabitants have access to the official Norwegian government-issued ID called «MyID», and many may in addition hold eIDs issued by the private sector. Once the user chooses an eID, the ID portal handles the authentication and communicates the result of the authentication to the relying party. This is done through an «SAML token»[53] that identifies the user (based on the national identification number) and includes information on the kind of eID used, as well as the assurance level of that eID.

52 To my knowledge, the current ID portal facilitates authentication only, but it is intended that future versions also will allow for functionality for signature and encryption.

53 In essence, the ID portal is uses SAML tokens using the Security Assertion Mark-up Language, an XML-based open standard for exchanging authentication and authorization data.

The latter is essentially a value between 1 and 4, where level 4 denotes the highest assurance an eID can offer.[54]

The governance framework for the Norwegian ID portal is based on contracts between the portal provider (the Norwegian eGovernment agency «Difi»[55]) and two sets of stakeholders, namely relying parties and eID providers.

First, there is the contractual relationship between Difi and eGovernment service providers—i.e., the relying parties. Any eGovernment service provider (such as the tax authority) wishing to use the ID portal needs to sign a standard «collaboration agreement» with Difi. This agreement not only includes the rights and obligations of the parties, but also lays down a basic governance framework for the eID portal. Overall, the governance of the ID portal is dominated by Difi, who finances the portal, retains the overall control over the portal and holds all rights. However, there are a number of collaborative organs with representation from relying parties. The highest degree of influence is vested on the «Advisory Board», formed by representatives from relying parties (selected by Difi). This board has a central role, *inter alia*, in advising on possible changes to the collaboration agreement. In addition, all relying parties may participate in the «Users Council», an organ that deliberates on issues prior to decisions of the Advisory Board. It should be emphasised that eID providers are not represented on the Users Council, but they can be invited to its meetings. In addition, there are other governance structures, such as the «Forum for Integration and Security» and the «Forum for User Support», and both can be attended by representatives from relying parties. The institutional framework put into place by the collaboration agreement is perhaps the clearest example of a governance model for interoperable eIDs. However, in order to assess the complete picture of this framework, we also need to take into account the roles of eID providers.

A second set of contractual relations exists between Difi and eID providers participating in the portal. These contracts were not available for the research purposes, but from publicly available information it is apparent these contracts were awarded following a request for proposals addressed to several eID providers. The requirements used to select eID providers seemed to have

54 This scale and the criteria for assurance levels regarding authentication and non-repudiation are defined in a an official guideline entitled «Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor: Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett», available at http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli.html?id=505958.

55 The Agency for Public Management and eGovernment (Difi), www.difi.no (last visited 10 November 2011).

emphasised both the eIDs' capabilities[56] and their assurance levels (on a scale from 1 to 4, as mentioned above).

Once an eID provider is granted access to the ID portal, the principle of non-discrimination applies. According to this principle, relying parties may not discriminate between eIDs that participate in the portal. In essence, relying parties may thus only select a required assurance level—based on their security needs asserted in a risk assessment—and if an eID provider fulfils these requirements, this eID provider cannot be excluded by that relying party.

10 Concluding remarks

Could this example of an eID portal be used as a blueprint for governing interoperability in Europe and beyond? It may be the case that existing eIDs in Europe are too heterogeneous to be incorporated in a single hub. However, this example illustrates fairly clearly that there are alternatives to creating a single and all-encompassing European eID if one wishes to facilitate interoperability in Europe.[57] Rather than offering European citizens and others yet another eID (for European use), we should consider the alternative of governing authentication processes based on a selection of existing eIDs. Of course, the model raises many new questions, such as who might establish such a portal, and how it should be governed. In my view, a governance framework for a potential European eID portal should go beyond the participative model selected in Norway and also encompass other stakeholders, such as eID providers, other intermediaries and perhaps also end-users and their representations in civil society organizations. Moreover, if the intention is to ensure eID interoperability also for non-governmental actors, the private sector should definitely be incorporated into the governance framework. The advantage of the eID hub model is its potential openness, which could potentially be used to encompass not only European eIDs, but perhaps even allow sufficient flexibility to facilitate interoperability with other non-European eIDs in the future. At the same time it has to be acknowledged that the model also may involve new legal challenges related to, for example, compliance and liability.

56 One applicant—the eID solution of the banking sector, bankID—was not awarded a contract because its eID solution did not facilitate encryption as specified in the requirements.

57 See Patrick Van Eecke's contribution in this issue.

11 References

Borges, G. „Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis: Ein Gutachten für das Bundesministerium des Innern.“ 2010, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/studie2_npa.pdf?__blob=publicationFile.

Bygrave, L. A., & Bing, J. *Internet governance: Infrastructure and institutions*. Oxford: Oxford University Press, 2009.

Clarke, R. «Identity management.» Xamax Consultancy, 2004, http://www.rogerclarke.com/EC/IdMngt-Public.pdf.

Cojocarasu, D. I. «Legal issues regarding WHOIS databases.» Oslo: Senter for rettsinformatikk, 2009.

de Andrade, N. N. G. «Towards a European eID regulatory framework. The legal gaps, barriers and challenges of constructing a legal framework for the protection and management of electronic identities.» In *European data protection: In good health?*, edited by S. Gutwirth, P. De Hert, R. Leenes and Y. Poullet. Springer, 2012 - forthcoming.

DeNardis, L. *Opening standards: the global politics of interoperability*. The information society series. Cambridge, Mass.: MIT Press, 2011.

Drake, W. J. «Introduction: The distributed architecture of network global governance.» In *Governing global electronic networks: international perspectives on policy and power*, edited by William J. Drake and Ernest J. Wilson. Cambridge, Mass.: MIT Press, 2008.

Froomkin, A. M. «Habermas@discourse.net: Toward a critical theory of cyberspace.» *Harvard Law Review* 116, no. 3 (2003): 749-873.

Hornung, G., & Roßnagel, A. «An ID card for the Internet-The new German ID card with ‘electronic proof of identity’.» *Computer Law & Security Review* 26, no. 2 (2010): 151-57.

Leenes, R., Priem, B., van de Wiel, C., & Owczynik, K. «D.2.2 — Report on legal interoperability.» Stork eID Consortium, 2009.

Lundevall-Unger, P., & Tranvik, T. «IP addresses–Just a number?» *International Journal of Law and Information Technology* 19, no. 1 (2011): 53.

Mueller, M. *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, Mass.: MIT Press, 2002.

Mueller, M., & Chango, M. «Disrupting global governance: The Internet WHOIS service, ICANN, and privacy.» *Journal of Information Technology & Politics* 5, no. 3 (2008/10/27 2008): 303-25.

Myhr, T. «Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution:: or I am 621216-1318, but I am also 161262-43774.1 Do you know who I am?» *Information Security Technical Report* 13, no. 2 (2008): 76-82.

Olsen, T. «Personvernøkende identitetsforvaltning.» University of Oslo, 2010.

Olsen, T., & Mahler, T. «Identity management and data protection law: Risk, responsibility and compliance in 'circles of trust'.» *Computer Law & Security Report* 23, no. 4+5 (2007): 342-51 & 415-26.

Pfitzmann, A., & Hansen, M. «A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.» version v0.34, 2010, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

Riisnæs, R. *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar: en tillitsorientert tilnærming til sertifikatutstederens villedningsansvar*. Bergen: Fagbokforlaget, 2007.

Thibeau, D., & Drummond, R. «Open trust frameworks for open government: enabling citizen involvement through open identity technologies.» In *White paper, OpenID Foundation and Information Card Foundation*, 2009, http://openid.net/docs/Open_Trust_Frameworks_for_Govts.pdf.

EN FORKASTET GOOGLE-AVTALE, ET UPOPULÆRT EU-DIREKTIV, EN NORDISK LØSNING - SAMT NOEN OPPHAVSRETTSLIGE UTFORDRINGER PÅ EUS DIGITALE AGENDA[1]

Helge Sønneland

Bakgrunn: Om Google-avtalen og hitteverk

I 2004 offentliggjorde Google sin plan om å digitalisere mest mulig av verdens litteratur. I Europa inngikk Google avtale med en del større universitetsbibliotek om digitalisering av litteratur som var falt i det fri – i USA ble avtaler inngått om å digitalisere også litteratur som hadde opphavsrettslig vern. Siden søkene i Googles bok-søk kun resulterte i små tekstutsnitt – «snippets» - mente Google at den digitale kopieringen måtte være tillatt under «fair use»-unntaket i amerikansk rett.

Googles initiativ utløste reaksjoner: På amerikansk side protesterte forfattere og forleggere, som gikk til sak mot Google i et gruppe-søksmål (class action). Høsten 2008 ble det inngått et forlik – den såkalte Google-avtalen. Etter kraftig kritikk ble den revidert, og en mindre omfattende avtale ble presentert november 2009. Den 22. mars i år ble avtalen forkastet av dommer Jeddy Chin i US District Court, Southern District of New York[2].

På europeisk side var det aldri tvil om at en digital kopiering krevde tillatelse enten fra rettighetshaverne, eller ved direkte unntak i loven, og at tilgjengeliggjøring krever avtale. Men Google-prosjektet imøtekom også et utstrakt ønske om å gjøre tilgjengelig kulturarven i digital form. EU-kommisjonen ga tidlig uttrykk for at en også på europeisk side burde få et tilsvarende prosjekt opp og stå – ikke minst for å kunne tilby attraktivt innhold i den utbygging av internett som var ønsket. «Europeana», en portal for europeisk kulturarvsmateriale i arkiv, museer og særlig bibliotek, ble svaret, og en rekke utredninger ble igangsatt.

En generell utfordring når det gjelder avtaler om digitalisering, er de såkalte «hitteverk» eller foreldreløse verk, hvor rettighetshaveren ikke er kjent

1 Også publisert i Nytt i privatretten, nr.4/2011.
2 Avgjørelse (05 CIV 8136), se www.nysd.uscourts.gov

eller ikke kan nåes. Søking etter rettighetshavere er administrativt og økonomisk krevende.

Google-avtalen løste dette med et svepende grep, ved å forutsette at dommer Chin godkjente at avtalen også ble gjort gjeldende for ikke-representerte rettighetshavere med mindre de – når det gjaldt bøker som ikke lenger var i handelen - aktivt meldte seg ut av avtalen.

I EU har spørsmålet om rettighetsklarering, og særlig hitteverk, blitt diskutert i flere år. EU-kommisjonens forslag til løsning ble lagt fram 24. mai 2011[3] – uten å ha vekket registrerbar begeistring så langt.

I de nordiske land er det unødvendig med en egen løsning for hitteverk på områder hvor loven tillater såkalt avtalelisens; at en avtale om bruk av verk av en viss kategori inngått med en representativ organisasjon i kraft av lovbestemmelsen utstrekkes til også å gjelde verk av samme kategori av ikke-representerte rettighetshavere. Det blir da opp til organisasjonen å finne fram til den eller dem som skal ha del i vederlaget, og noe forhåndssøk er ikke nødvendig. I slike avtaler kan det tas inn bestemmelser om rett til å melde seg ut av avtalen. I Norge er det inngått en avtale mellom Kopinor og Nasjonalbiblioteket om pilotprosjektet «Bokhylla.no», hvor 50 000 beskyttede bøker utgitt i bl.a. perioden 1990-1999 gjøres tilgjengelig over nett for lesing. Avtalen går ut 31. desember 2011 og evalueres nå.

Google-avtalens skjebne

Hitteverk-problematikken og spørsmålet om avtalens utstrekning til også å omfatte alle som ikke hadde meldt seg ut, sto sentralt i avgjørelsen til dommer Chin. Den opprinnelige avtalen omfattet alle litterære verk i bøker (men ikke illustrasjoner) som fantes i magasinene til de samarbeidende bibliotekene. Dette omfattet ikke bare bøker utgitt i USA men også en stor del europeisk litteratur! Google skulle betale 125 mill. US dollar, og honorar pr scannet bok var satt til 60 dollars. 34 mill. dollars skulle gå til etablering av et bokregister – reelt sett en forvaltningsorganisasjon – som skulle kunne inngå avtaler med om videre utnyttelse av det digitaliserte materialet. Forleggere og forfattere var jevnt representert. Google fikk rett til å selge lisenser, og 63 % av fortjenesten skulle tilfalle rettighetshaverne. For bøker som ikke lenger var i salg, måtte opphavsmannen aktivt melde seg ut for ikke å være omfattet. For bøker i salg måtte opphavsmannen bekrefte sin medvirkning.

Protestene fra Europa var massive med påstander om at avtalen var i strid med internasjonale forpliktelser. Avtalen ville også gi Google et *de facto*-mono-

3 Com (2011) 289 final

pol, ble det hevdet. Avtalen ville også gi Google en løsning på spørsmålet om hvem som egentlig hadde de digitale rettigheter til en bokutgivelse – noe andre aktører ikke ville kunne oppnå. Det amerikanske justisdepartement fremholdt også med styrke at avtalen ikke ble dekket av bestemmelsen om godkjenning av minnelige løsninger i gruppesøksmål (den føderale sivilprosesslovens regel 23).

I den reviderte avtalen av 2009 var avtalen redusert til å omfatte bøker registrert i USA, eller utgitt der, i Storbritannia, Canada eller Australia. Det var også lagt opp til fondsavsetninger for vederlag til hitteverk, og utenlandske rettighetshavere skulle være representert i bokregistrets styre.

I perioden fram til dommer Chin offentliggjorde sin beslutning, kom det fortsatt mange innsigelser. For at avtalen skulle kunne gå inn under regel 23, måtte avtalen bedømmes som «rettferdig, adekvat og rimelig» (fair, adequate and reasonable). Det fant dommer Chin at den av flere grunner ikke var. Et hovedankepunkt var at avtalen omfattet tillatelse til tilgjengeliggjøring og salg av de digitaliserte verkene – en bruk som lå langt fra det den opprinnelige rettssaken gjaldt, nemlig den første digitale kopiering. Det var urimelig å la den gjelde også for alle som ikke aktivt meldte seg ut. Her var dommeren enig med de amerikanske myndigheter; dersom avtalen skulle kunne utstrekkes på denne måten, var det en sak for lovgivende myndigheter. Dommeren noterte også påstandene om brudd på internasjonale avtaler – igjen et tema som passet bedre for Kongressen å ta stilling til, enn for en dommer. Det faktum at Google, ved å ta seg til rette, gjennom avtalen ville sikre seg en *de facto*-monopolsituasjon når det gjaldt bruk av hitteverk, talte også imot å godkjenne avtalen. Han la til at han ville sett langt mer positivt på avtalen hvis den hadde vært basert på at man «meldte seg inn» (opt-in) heller enn å måtte melde seg ut (opt-out).

Hva nå? Det er uklart i skrivende stund, men mye tyder på at det kan gå mot rettssak Dommer Chin (som underveis er forfremmet til en føderal appelldomstol, men likevel beordret å sluttføre saken i distriktsdomstolen) ga først partene frist til 1. juni 2011, senere 17. juli, til å finne en løsning – men noen ny avtale er ennå ikke inngått. Det har vært et status-møte 15. september, og dommer Chin traff der beslutning om en tidsplan fram til beslutning. ..Planen forutsetter at partenes forslag til ny avtale er klar innen utløpet av mai ,og at alle innsigelser og tilsvar er lagt fram innen 31.juli 2012. Et krav om å «melde seg inn» vil utvilsomt gjøre færre verk disponible, og Google har uttrykt negativ holdning til dette alternativet.. Rapportene etter møtet tyder på at forlegger-siden er mer positive til å finne en løsning med Google enn forfatterne. Dette kan resultere i at forfatterne går videre mot en rettssak. Illustratører og fotografer har tatt ut stevning mot Google, og disse vurderer å kjøre en parallell rettssak. Disse gruppene var utelukket fra den opprinnelige avtalen siden illustrasjoner ikke skulle inngå i forliket). Også australsk forfatterforening

og forfatterforeningen i Quebec har gått til søksmål. I mellomtiden fortsetter Google sin digitalisering, og har så vidt det fremgår av dommen av mars i år nådd opp i ca. 12 millioner digitaliserte bøker!

Så kan man spørre: er det ikke sterke likheter mellom Google-avtalen og de nordiske lands avtalelisensløsning? Jo - for så vidt som man i begge tilfelle lar en avtale mellom bruker og rettighetshaverorganisasjoner utvides til også å gjelde verk av ikke-representerte rettighetshavere. Men på to avgjørende punkter er det forskjell; det ene er at lovgiver har tatt stilling til når og under hvilke forutsetninger en avtale om bruk av verker kan utløse avtalelisensvirkning. Det andre er at lisensvirkningen kun blir aktuell dersom det foreligger en frivillig fremforhandlet avtale mellom brukeren og rettighetshaverne.

De nordiske avtalelisensløsningene er i utgangspunktet nasjonale. Spørsmålet er hvordan rettighetsklarering også av hitteverk kan gjøres grenseoverskridende. Nasjonalbibliotekar Vigdis Moe Skarstein har foreslått at de nordiske land avtaler å godkjenne hverandres avtalelisensordninger. Kulturminister Anniken Huitfeldt har tatt opp spørsmålet i Nordisk ministerråd, og saken utredes nå der.

EU-direktiv om hitteverk

Det er spørsmålet om grenseoverskridende virkning EU-kommisjonen tar sikte på å løse i det direktivforslag den la fram 24. mai 2011.(COM(2011) 289). Forslaget er en del av den digitale agenda, og inngår i en plan om å styrke det indre marked – ikke minst å utvikle ett, digitalt indre marked.

Etter forslaget får museer, arkiv og bibliotek adgang til å gjøre tilgjengelig hitteverk i trykte skrifter som bøker, aviser, tidsskrifter mv. som de har i sine samlinger, inklusive illustrasjoner som inngår, dersom de har gjennomført et grundig (diligent) søk etter opphavsmannen. Den samme rett har allmennkringkastere med hensyn til sine arkiv (for produksjoner laget før 31.12.2001), og nasjonale filmarkiv. Om de ikke finner rettighetshaveren, skal verket og søket registreres i offentlig søkbare registre. Det er opp til medlemslandene å fastsette krav til søk, men direktivet gir visse minimumsbestemmelser. Søket skal foretas i første utgivelsesland. Verk som etter dette er erklært som hitteverk gis tilsvarende status i hele EU-/EØS-området. En opphavsmann kan til enhver tid melde seg og dermed oppheve verkets status som hitteverk.

For den bruk som gjøres innenfor disse institusjonenes allmenne formål, skal det ikke betales vederlag. Bestemmelsene blir m.a.o. en bestemmelse om unntak fra opphavsmannens enerett. Dersom det gjøres bruk av verket på annen måte (f.eks. i kommersiell sammenheng) skal det betales vederlag. Direktivet gir anvisning på anvendelsesformål for midler som ikke kan utbetales.

I punkt 20 i fortalen heter det at direktivet ikke skal ha innvirkning på «eksisterende» ordninger for forvaltning av rettigheter i medlemslandene, så som avtalelisenser. Det er uklart hva dette innbærer - om det både gjelder enkelte avtaler, eller bare muligheten til å innføre nye lisensordninger. Det er med andre ord konflikt mellom direktivet og de nordiske lands ordninger og deres ønske om å stå fritt i intern lovgivning.

Når kommisjonen avviser den nordiske modell som en løsning, er det fordi den ikke krever forutgående søk.

De reaksjoner jeg har registrert til nå er – ut over negative reaksjoner i nordiske land på fortalens punkt 20 - ikke positive: Fra bibliotekshold blir det påpekt at direktivet kan komme til å medføre unødvendig byråkrati. Hitteverks-problemet er viktig nok, men deres hovedanliggende er å få avtaler om digitalisering og tilgjengeliggjøring av vernet litteratur som ikke lenger er i handelen.

Rettighetshaverne reagerer særlig på at det ikke skal betales vederlag, og ønsker å erstatte unntaksbestemmelsen med krav om avtale med relevant rettighetshaverorganisasjon.

Flere stiller av denne grunn spørsmål ved om direktivet kan være i samsvar med medlemslandenes forpliktelser etter Bern-konvensjonen og TRIPS-avtalen og viser til den såkalte tretrinns-testen. Den forbyr å innføre bestemmelser om unntak fra eneretten med mindre det gjelder særskilte tilfelle som ikke strider mot den vanlige bruk av verket, og som ikke på urimelig måte strider mot rettighetshaverens legitime interesser.

Som bibliotekene påpeker, løser med andre ord direktivet ikke deres hovedutfordring. Når det gjelder bøker som ikke lenger er i handelen, er det oppnådd en forståelse mellom partene – forfattere, forlag, rettighetshaverorganisasjoner og Kommisjonen – om en intensjonsavtale (Memorandum of Understanding) om tilgjengeliggjøring. Her har man lagt til grunn at en rettighetshaverorganisasjon på visse vilkår kan presumeres å representere også ikke-medlemmer, noe som krever nasjonal lovgivning. Etter min oppfatning vil det, for å oppnå grenseoverskridende effekt av en avtale, kreve EU-lovgivning, noe som indirekte fremgår av memorandumet.. Normalt burde dette dokumentet få konsekvenser for forhandlingene som nå pågår om direktiv-forslaget, og resultere enten i en utvidelse av direktivets virkeområde eller et ytterligere forslag. Imidlertid kan det synes som det polske formannskap setter alt inn på å få en avgjørelse om direktivet innen årets utgang – noe som forutsetter at innsigelsene ikke blir for store. Mange bedømmer denne tidsplanen som urealistisk.

IP-strategi i EU

Forslaget om hitteverk er en del av den digitale agenda, som Kommisjonen la fram i fjor. Det inngår også i en plan for opprustning av digitale indre marked.

Med sikte på dette la Kommisjonen fram en strategi for hele immaterialrettsområdet den samme dag som hitteverk-direktivet ble lagt fram (COM(2011) 287).

Blant de tanker jeg har notert meg, er at man på sikt ser for seg en felles europeisk opphavsrettslov. En begynnelse ligger naturlig nok i kodifisering de gjeldende direktivene. Kommisjonen mener det kan være fornuftig å begynne en slik prosess i 2012 ved å se på unntakene fra eneretten, og stille spørsmål ved om det er ønskelig med ytterligere harmonisering. En bakgrunn for dette er at en gjennomgang av hvordan medlemslandene har gjennomført det såkalte Informasjonssamfunnsdirektivet fra 2001 (direktiv 2001/29/EF), viser at harmoniseringen i stor grad gjelder rettighetene – og i svært liten grad unntakene. Dette har igjen skapt problemer i digitaliseringsarbeidet.

Kommisjonen tenker seg også muligheten av at man kan få en lov om opphavsrett som gjelder for hele EØS-området.

Disse tankene følges opp i Kommisjonens seneste utspill fra 17. juli 2011 (COM(2011) 427), som kom i form av en grønnbok om online distribusjon av audiovisuelle verker, hvor man ønsker debatt om disse spørsmålene, med frist for å komme med innspill 18. november 2011. Man vil gjerne identifisere hindringer for det indre digitale marked, og gir – igjen – uttrykk for sin bekymring over hvor vanskelig det er å få klarert rettigheter for hele eller større deler av det europeiske territorium. Kommisjonen reiser spørsmål om det bør innføres en ordning når det gjelder online distribusjon av audiovisuelle verker basert på løsningen i direktivet om satellitt- og kabelsendinger, nemlig at avtale inngås i senderlandet, og at man der tar hensyn til spredningen i andre land. Kommisjonen reiser også spørsmål om det bør bli mulig å erverve en (frivillig) europeisk opphavsrett parallelt med nasjonal rett, og om hvordan dette i så fall kan gjøres. Dokumentet stiller også spørsmål om behov for harmoniserte unntak til fordel for funksjonshemmede og til fordel for nasjonale filmarkiver. Det er m.a.o. klart at tiden fremover vil by på mange spennende opphavsrettslige utfordringer som har relevans også for EØS-avtalen.

DEVELOPING EGOVERNMENT SYSTEMS – LEGAL, TECHNOLOGICAL AND ORGANIZATIONAL ASPECTS[1]

Dag Wiese Schartum

1 Approaching eGovernment

Government administration of Nordic countries is comprehensive and plays a central role in the provision of welfare to citizens. Government agencies both exercise authority and produce services through a diversity of schemes. From the start of the 1960s and, in particular, during the last fifteen years, government administration has been transformed into machine-managed, electronic government (eGovernment). In this respect the Nordic countries today are among the most advanced in the world. In a United Nations ranking of e-readiness, Sweden, Denmark and Norway held the top three rankings.[2] Highly developed eGovernment sectors have developed concurrently with the high degree of access to Internet enjoyed among citizens. In 2009, 86 % of the Norwegian population had access to Internet and 73% had access to broadband, implying that the current level of technology infrastructure allows comprehensive and advanced electronic interaction between government and citizens. Moreover, 81% of the Internet users communicated via the Internet with the government sector during the last twelve months.[3]

My aim in the following pages is first and foremost to demonstrate and discuss interrelationships between legal, technological and organizational aspects of eGovernment. I use Norwegian eGovernment as an example. My intent is to convince readers that successful development of future eGovernment administration requires an integrated approach since the traditional professional

---

1 Previously published in *Scandinavian Studies in Law*, 56, s. 125-147.

2 Cf. UN E-Government Survey 2008. From e-Government to Connected Governance, United Nations, New York, 2008, table 3.1. The e-government readiness index combines the UN's web measure index, telecommunication infrastructure index and human capital index. The survey focuses mainly on the government- to-citizen and government-to-government aspects of e-government, but only to a very limited extent on the relations between government and business.

3 Source: Statistics Norway, http://www.ssb.no/ikt/.

areas (ICT, law, and organization) are in a continual process of communication, interaction and mutual influence. I will not, however, delve into the many faceted issue of how relevant national laws should be understood in the context of ICT in a reorganized government administration, but will instead investigate how the aforementioned professional elements are and should be connected.

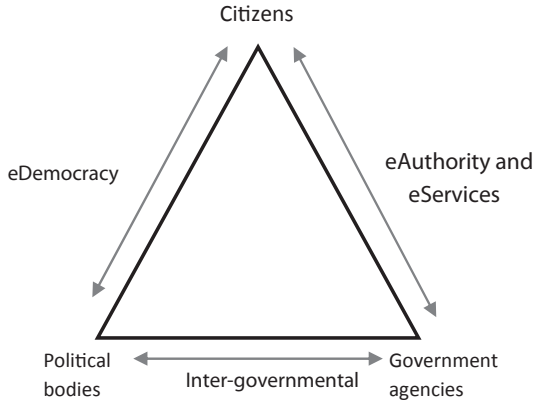


Figure 1: Main actors and relations in eGovernment

eGovernment is a wide concept covering both democratic and administrative aspects. Here, administrative aspects will receive the greatest attention, meaning that I will not discuss questions regarding representative democracy (electronic elections etc, cf. left-hand side of figure 1.) There are, however, important democratic elements embedded in administrative sides of eGovernment too, for instance regarding access to government-held information and public hearings on proposed new legislation. Primary focus will be on the relationship between government agencies on the one hand and citizens on the other. Citizens embody at least three roles: as members of the public, as data subjects and as parties to individual cases. Emphasis will be on the role as party because this role comprises the two others. Aspects of inter-governmental management, i.e. political and administrative steering and control in and between political bodies and government agencies (cf. bottom line of figure 1) will only receive attention to the extent it is relevant for the exercise of authority and services (cf. right hand side of figure 1).

eGovernment has been defined in many ways, and different definitions accentuate different possible elements.[4] Twenty years ago and earlier, before the use of word processing and other ICT-based office support tools became common, it was meaningful to distinguish between electronic and (purely) manual government. Today the use of various electronic tools is commonplace, and all government agencies use word processing, email and web-services. Meaningful use of «eGovernment» should thus probably be reserved to ICT applications of more advanced nature. How advanced and in what way ICT applications are to be used, however, is an open question. At least four main characteristics may be identified, in my view, as particularly relevant for the purposes of this article: eGovernment typically handles electronic *documents* as sources of information; they *communicate* by means of ICT; they execute *automated operations* by means of programs developed to execute their specific tasks; and they typically generate an electronic *track of activities* (by means of logging etc). The more relevant the mentioned characteristics are, and the more important they are, the higher the need for an eGovernment concept to signal requirements for reflection and discussion. Here, I choose to use rather advanced eGovernment as an example, that is, government bodies integrating all of the four technological characteristics mentioned.

Definitions of eGovernment often signal political means and ambitions. A rather technology-specific and detailed definition of eGovernment is found in the US Electronic Government Act:

> *«The use by the government of* ***Web-based Internet applications and other ICTs****, combined with processes that implement these technologies, to a) enhance the access to and delivery of government information and services to the public, other agencies, and to government entities; or bring about improvements in government to operations that may include effectiveness, efficiencies, service quality, or transformation.»* [5] *(Emphasis added)*

«Other ICTs» (cf. quotation) may be read as a reminder that use of information technology in the government sector started fifty years ago. «Web-based Internet applications» have brought technology out into the public sphere and citizens have assumed the role of users of ICT which previously was reserved for internal government use. Words like «enhance», «improvements» and

4 Several definitions and examples are presented in Michael Chissick and Justin Harrington (eds.), «E-Government. A Practical Guide to the Legal Issues», Thomson, London 2004, pp 4 -11.

5 US government (2002) The e-government act of 2002. HR 2458, "§ 3601. Definitions (3), se http://csrc.nist.gov/drivers/documents/HR2458-final.pdf.

«transformation» signal positive change as the overall goal, and service access and quality, effectiveness and efficiency are set as areas of change. Thus, this definition of eGovernment does not express «business as usual» but «better business». Descriptions of aspired improvements donot, however, express typical legal goals, but are rather marked by mindsets of economists and businessmen.

Other definitions of eGovernment are made technologically neutral and in addition introduce clear organizational elements:

> *«eGovernment is defined here as the use of ICT in public administration* ***combined with organisation changes*** *and new skills in order to improve public services and democratic processes and strengthen support to public policies.»*[6] *(Emphasis added)*

The need to combine ICT and organizational development is generally recognized and well established, and reflects the idea that both «production conditions» and outputs should undergo change. Reformed technology and organization, in other words, creates new skills for the benefit of citizens and private agencies etc.

If customary business thinking dominates our understanding of eGovernment, it is easy to forget the special features of government administration. One important characteristic is that democratic governments are built on the idea of the constitutional state and the principle of rule of law. The Norwegian government sector, furthermore, is ruled by statutory law to an almost extreme degree. Our government administrative law contains great compilations of (often) very detailed rules regarding subject matter and procedure in various decision-making processes. eGovernment may thus be described as an area where legal regulations play a very significant role. Thus, one may ask why changes brought about by *the legal system*, in particular statutory law, are not part of the change processes embedded in the cited definitions.

One of the fundamental insights of this article is that changes brought about by the legal system should be seen as typical elements of eGovernment considerations, similar to the qualification of organizational change. I claim this as a prerequisite for the improvement of outputs from government agencies: The aim should be not only to improve services, efficiency etc, but also to

6 COM (2003) *The Role of eGovernment for Europe's Future*. Communication from the Commission to the Council COM (2003) 567 Final, para 3. Brussels 26.9.2003, se http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf.

ensure correct individual decisions, protection of personal and business data etc. The legal system is in itself dynamic. Statutory law is continually amended to catch up with and impel changes in society; courts and administrative bodies of appeal clarify applicable law etc. It is thus impossible to attempt to preserve the architecture and subject content of eGovernment systems. Even organizational structures may be heavily influenced by legal change.

This article emphasizes elements of change in the eGovernment sector and underscores that legal, technological and organizational change must be seen as three integrated change processes (cf. figure 2). The objective of such alterations is to improve the results of government activities. Because government agencies exercise authority in individual cases, improvements should also embrace legal decision-making. Legal elements should be present on both sides of the definition of eGovernment; as a measure (in line with new ICT and reorganization) and as an aspired result (in line with improved services, efficiency etc). I designate such positive and controlled change processes in eGovernment as a «development», implying that the three central change processes of electronic government could be identified as developments of ICT systems («system development»), organizational development and regulatory development. I use «eGovernment system» as a common designation of the output from such integrated development processes. The eGovernment system does not, in other words, refer only to technological aspects of information systems, but also includes integrated organizational and juridical elements.

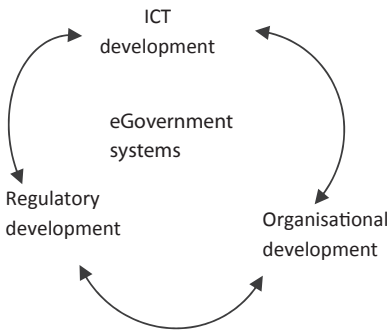


Figure Main different development aspects of eGovernment systems

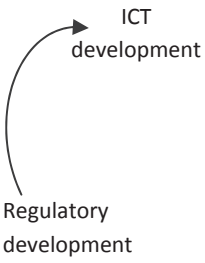
This triangular approach to eGovernment both recognize the three elements and - just as importantly – take into account the relationship between them. The development processes could/should influence one another in both direct and indirect ways. Below emphasis will be on such direct and indirect influ-

ences. Indirect effects, for instance, may occur if organizational change makes changes in ICT necessary, which again triggers regulatory amendments. To what extent and in which ways the three development processes influence one another directly or indirectly is a factual/empirical question, but is also a matter for normative considerations: How *should* system development influence regulatory development and vice versa?

2 Regulatory development and ICT systems

2.1 Introduction

Government sector is – as stated earlier –heavily regulated by statutory law. eGovernment implies on the other hand that these laws are handled by means of ICT: Certain legal rules regulate, for instance, the handling of electronic documents, how electronic communication may be carried out, and to what extent and on what grounds government may keep track of their activities by means of logging etc. The doctrine of sources of law and legal principles, moreover, are crucial in cases where government wishes to transform statutes and other legal sources into computer programs, in order to be able – wholly or partly – to automate application of the law. Development of ICT systems in government administration is in other words based to a large extent on law, and influenced by law, in a very direct and comprehensive manner.



This legal environment to which eGovernment is so tightly connected is of a dynamic nature. Thus, amendments of acts and regulations, as well as new judgements and administrative practices, represent sources of legal change which may create the need for corresponding changes in ICT systems. Some changes are easy and inexpensive to implement. However, eGovernment information systems are rather intricate and are therefore challenging to update pursuant to legal change. One important objective of developing eGovernment, moreover, is to improve interoperability between government agencies, implying that information systems are linked together and partly integrated, creating complex connections. Integration may imply that amendments in one piece of legislation entail the need to change interconnected information systems of other

government agencies as well.[7] Viewed from an information system perspective, the dynamic nature of law is rather unpleasant and expensive and could potentially damage and even disintegrate beautifully designed systems and models.

eGovernment and development of information systems are influenced by law in two main ways. Firstly, law is the framework of information systems, that is to say, statutory law, judgements, etc. must be observed when information systems are planned, designed and realized. Such rules are relevant, but not necessarily subject to automation and transformation into programming code. Certain bodies of general legislation will almost always be relevant for the development of eGovernment information systems. The Public Administration Act (PAA), Personal Data Act (PDA), Freedom of Information Act (FIA), and Archives Act constitute comprehensive standard legal frameworks for every government activity involving exercise of government authority, including when facilitated by ICT.

Secondly, there will almost always be a comprehensive special statutory regulation concerning the government scheme in question (e.g., within tax and duties, social benefits, admission to public services, etc). Such rules regulate contents and procedures specific to each type of government decision in individual cases, for example on what conditions taxes and benefits are established, legally correct factual bases and processing of these facts, etc. Such rules will typically be transformed wholly or partly into programming code and will be subject to automatic processing, cf. 2.3 (below).

2.2 Law as a framework for information systems

Classification of law as a «framework» includes at least two observations. Firstly, it means that legislation contains boundaries that may not be transgressed. Secondly, it indicates a type of legislation which is difficult to transform and represent as programming code in the system. For instance, section 17 of the PAA regarding the administrative agency's duty to clarify cases, states that «the administrative agency shall ensure that the case is clarified as thoroughly as possible before any administrative decision is made.» Such highly discretionary rules are not possible to transform into programming code[8] but may be substituted by a very high number of fixed rules.

7 This may be the case, for instance, if several agencies establish joint use of information based on the fact that a definition of concept is equal in two or more Acts. If definitions are changed by amendment or judgment, this may cause a rethinking in all agencies using that common piece of information.

8 At least not by means of standard programming languages and logic.

The situation that «framework legislation» for eGovernment functions may not be subject to automation does not, however, imply that application of such legislation may not be subject to eGovernment *support* systems, that is, information systems designed for distribution of legal information and manual operation. Access rights of the PAA, DPA and FIA may for instance be supported by internet-based access request routines which present information regarding access rights and facilitate access requests.[9] If legislation alters the right to request access and makes it an obligation to make information *accessible* by ICT, it would, however, be possible to partly automate freedom of information laws too.

2.3 Law as contents of information systems

Special statutory regulations concerning each government agency's tasks and responsibilities, in contrast to the described framework legislation, are often quite easy to transform into programming code and make subject to automated application of the law.[10] Standard transformation approaches create a tension between the legal sources which are basis for the process on the one hand, and the formal representation of these sources (programming code) on the other. Transformation is dependent on the logical repertoire and expressiveness of standard programming languages. Thus in the course of transformation processes, the task is to understand legal rules in ways which may be expressed by means of programming languages. Deontic logic[11] and discretionary rules lie outside what such standard languages are capable of expressing, and therefore these rules must be either omitted[12] or transformed into similar rules which a standard programming language may express.

Other tensions between the legal sources and their representation in eGovernment systems are due to the imperfectness of many statutory texts. Statutes are written in «natural language» (as oppose to formal langue). When natural languages are used to express formal operations, for instance strictly mathematical and logical operations, it is difficult to express these operations in a

9 See for instance the public electronic government files system [offentlig elektronisk postjournal] (http://www.oep.no/nettsted/fad) which gives access for everybody to search in and order government-held documents from a common, complete filing system with documents of central government agencies (ministries, directorates etc.).

10 The dominating perspective of transformation of law in the eGovernment sector is characterized by a procedural approach using standard programming languages. More advanced approaches based on deontic logic and/or simulation of professional legal reasoning, do not play a significant role in current eGovernment systems.

11 Cf. «shall», «can», «ought to» etc.

12 And handled manually.

100% clear and unambiguous manner. Thus transformation processes will often reveal lack of stringency in the wording of statutory texts.

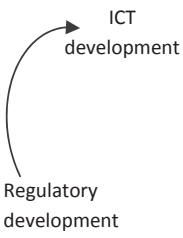
Lack of clarity concerning how formal operations shall be carried out will almost never have rational reasons. The intention of the lawmaker, for instance, is almost always to express calculations of taxes and benefits, etc. in an unambiguous way, and there are never, or very seldom, rational reasons leaving doubt as to whether or not conditions are cumulative or alternative. Stringency requirements also have effects for choice and variation of words and expression. In imaginative literature, linguistic variation and inventiveness is an important quality. By contrast, «statutory prose» requires consistency in the use of terms in order to avoid unnecessary problems of interpretation. Thus legislators should not vary terminology by using synonymous expressions such as «income», «earnings» and «earned income» in the same statutory text unless these words express different subject matters. Transformation processes reveal possible incidents of unmotivated linguistic variation and lead to standardization in the ICT system accordingly.

Both types of the mentioned tensions between legal sources and their formal representation in programming code may be starting points for discussions on the extent to which governments need methods and tools in order facilitate bridge-building between the legal and the ICT sides of eGovernment. Below I will address selected parts of this question.

3 Development of ICT systems and the law

3.1 Introduction

It follows from the Instructions for Official Studies and Reports of the Norwegian government system, that administrative and economical consequences of, for example, novel/amended legislation should be investigated and clarified.[13] This obligation of committees of inquiry, etc. is not given much attention in the committees, and frequently these types of issues are superficially discussed on one page towards the end of very extensive reports. One of the reasons for this perfunctory treatment is obviously that the political subject matter is considered far more important than potential administra-



13 See Utredningsinstruksen [Instructions for Official Studies and Reports] of 18 February 2000, amended 24 June 2005, section 2.1.3.

tive consequences. This is also true in most cases of law reform within the eGovernment area, for instance when laws to be transformed into programming code are introduced or amended.

Members of expert committees are nominated because of their competence within the specific areas of policy/law, and not because they know much about administrative and technological consequences for eGovernment systems. Possible administrative effects are difficult to assess because methods and tools to carry out such assessments are lacking. Thus, predictions of possible effects are very uncertain. Thirdly and most importantly is the fact that the legal-political process and the budgetary-political process are separate processes. Effects of proposed legislation are often dependent on sufficient measures to implement the rules, while questions of acceptable appropriation are outside the legislative process. In other words, there is little incentive for participants in the legal process to try to specify the administrative and technological conditions, effects and appurtenant costs.

The Instructions for Official Studies and Reports do not have a specific eGovernment perspective. The general underlying assumption is simply that novel legislation may require additional or fewer staff members, reorganization, development of new routines and systems (including ICT-systems) , etc. If administrative consequences of proposed amended legislation regarding new or considerably changed ICT-systems were to be more than «guesstimates», much work on system requirement specification etc. would have to be part of the work carried out by committees of inquiry. However, as mentioned, such committees only scratch the surface of administrative, technological and economical challenges, with the result that legal aspects are by and large decided with little more than elementary and uncertain thought given to how they should be implemented in existing or new information systems and at what cost.

The fact that legal considerations come first while assessment of administrative and technological consequences and the like is neglected, entails the subsequent need for government administration to rethink the legal solutions once they reach the process of implementation by ICT. Thus, legal considerations are not exhausted merely because a piece of legislation passes; they continue as part of the development processes required to put the laws into force. There are, however, at least two very important differences between the first type of legal consideration and similar considerations as part of system development processes:

Committees and government departments proposing new/amended legislation have primarily a political perspective with special attention to principles and overall solutions in subject matters. Focus is on fair and balanced legal and political solutions in accordance with legal and political principles, etc.

People working to implement passed legislation, by contrast, are motivated by an approach wherein detailed solutions and nooks and crannies in adopted legal provisions are scrutinized closely. Legislators are concerned with policy issues like «how can we treat live-in partners equally with spouses», while system developers are more occupied with questions like «do couples qualify as live-in partners if they temporary live separately because one of them is in prison?». Systems developers may experience their fate entails trying to tackle the open questions and «stupidities» left unaddressed by the legislators. Thus legislation may easily be seen as an obstacle to the «best» and rational ICT and organizational solutions.

3.2 Why can't regulatory development follow ICT requirements?

Law is often seen as a constraint in the development of information systems of electronic government, and the observation is apt, because law is often *indented* to be a constraint – not for the development of information systems in particular – but for exercise of government authority. One of the core qualities of the constitutional state is that the legislator is bound by their rules, entailing that they cannot change taxes or remove benefits without amending legislation. Most people would probably agree that the use of ICT-systems to implement such laws should not weaken this fundamental protection of citizens.

There are, however, different degrees of legal change, and even though everybody probably would agree that eGovernment projects should not be allowed to entirely repeal or introduce legal rules, disagreements may increase if we regard the various detailed sub-elements of binding regulations. Legal rules applied by government agency A, for instance, may rest on how the phrase «couples living together in marriage-like relationships» should be understood. Before introduction of eGovernment systems, for instance, legal custom and usage was to consider the question case-by-case. If government agency B possesses a database containing information regarding people recognized as «live-in partner» pursuant to a different part of legislation, it may seem obvious to systems developers that agency A should use information from agency B. Such changes will probably reduce costs and speed up case-processing. If the understanding of «couples living together in marriage-like relationships» and «live-in partner» is identical, there are probably no subject legal obstacles for A to access B's information. If, on the other hand, correlation between definitions is less than 60%, it is obvious that agency A should not be allowed to base decisions (only) on agency B's information.

But what if definitions were almost identical: 95 or even 98%? This may imply in concrete figures that 200 of 10 000 people would have the classifi-

cation of their non-marital cohabitation changed, with possible direct consequences for their legal rights or duties. In other words, safeguarding the legal protection of 200 people could prevent the use of rather inexpensive technological solutions that would improve the processing of almost 10 000 cases. If the rights or duties of the 200 were to be changed through a statutory process, it would require time-consuming (and expensive) procedures of statutory amendment.

The point is that legal implications of new and more rational eGovernment systems may be comprehensive or minimal or everything in-between. Most of us will agree that total and considerable change of legal rules through design of eGovernment systems would be unacceptable, and that parliamentary procedures of amendments would have to apply. The more limited the desired changes in systems development is, in terms of number of people and individual effects, the less serious the changes are from a pragmatic perspective. However, in principal even unauthorized change with negative effects for *one* citizen would be inacceptable.

The next possible legal constraint in example of the live-in partner is the situation that – even though definitions are identical –agency B is prohibited from providing agency A access due to the statutory mandate of nondisclosure. These types of access constraints may be introduced for many reasons. In most cases privacy protection is the simple and obvious reason. Sometimes nondisclosure protects data quality because it is recognized that people would be more frank if access to information is limited. Restricted access may also be introduced at the time of enactment because it gilds the pill of a controversial reform because it restricts the knowledge and potential powers of a government agency. Some people may even think of themselves as the rightful «owners» of information pertaining to them, and would thus claim a right to be in control of how personal information is dispersed.[14]

Only the very naïve would expect legislation to be 100 % rational and defendable. Development of information systems may often reveal more or less obvious needs for amendments, with the aim for instance to introduce more effective ICT-procedures and cut time of procedure. Some needs of amendments identified in course of systems development collide with explicit political grounds as expressed in preparatory works of laws, in court decisions etc. Others exist unexplained or with only vague substantiation. The fact that explicit grounds are missing, should not necessarily be read as a confirmation

14 See Dag Wiese Schartum: «ICT, service policy and changed division of work between citizens and government: towards a distributed, user-monitored government?» Electronic communication law review 2002; 9(1):7-22.

that no such motivation exists. In many cases, however, it should expected that no single important political or legal consideration should determine one specific solution, and that another more efficient and equally fair solution may be chosen instead.

Table 1: Definitional conditions of «live-in-partner» identified in four Norwegian laws.15

Category	Conditions	Act no.
Personal	More than 18 years old	1
Accommodation	Joint address	2
	Joint accommodation	4
	Living in the same house with less than four separate accommodations	3
	Temporarily apart	3
	Temporarily apart excluding imprisonment	2
Life together	Stable and established relationship as live-in partners	1
	Intention of continuing to live together	1
	Joint housekeeping	2
Duration	Of live-in partnership	1
	Of relationship similar to marriage or registered homosexual partnership	4
Children	Are parents to joint children	1, 3, 4
	Have been parents to joint children	3
Marriage etc	Have previously been married	3
	Marriage would have been legal	1, 2, 3, 4
	Registered homosexual partnership would have been legal	2, 4

Examples from Norwegian laws defining couples living together in marriage-like relationships may illustrate the point (cf. table 1). The tables show various definitional elements of «live-in partner» pursuant to four Norwegian Acts of Parliament.[16] I have grouped elements under six categories to make comparison easier. Several of the elements are very similar, for instance «joint

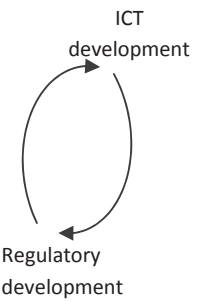
15 Cf. Dag Wiese Schartum, *Sharing information between government institutions - Some legal challenges, i: van der Hov and Groothuis (eds.) Innovating Government, Information Technology and Law Series vol. 20*, Springer 2011.

16 Act concerning the entry of foreign nationals into the Kingdom of Norway and their presence in the realm, Act on Norwegian nationality, The National Insurance Act, and Act concerning individual pension agreements.

address» is very similar to «joint accommodation», and «temporarily apart» is very similar to «temporarily apart excluding imprisonment». The point here is not to claim that these differences lack rational grounds. It is very likely, however, given a situation where information systems may be improved, that many such definitional elements could be coordinated at very little or no political or legal cost.

The general point is that transformation of legal sources into programming code in information systems makes it impossible to accept transformation as a one-way process from law to ICT system. Without feedback processes legal bases would be accepted as it is. There are at least two reasons, however, why the legal basis often should be changed:

a. Several elements of legislation are not or are only partly based on in-depth analyses and grounds, and are thus relatively open for amendment (definition 2 of «live-in-partner» may be just as acceptable as definition 1).
b. Even elements of legislation which are established on basis of solid analyses and grounds may be open for amendment provided sufficiently strong new arguments, e.g. regarding eGovernment needs.



Intended legal constraints as mentioned above are of category b. They are not untouchable, but may be politically controversial.

These potentials for change are related to what may be seen as weaknesses of the legislative process (cf. section 3.3 below), and the fact that detailed elements of legislation may be seen as accidental occurrences and intuitive solutions. When conditions like «joint address» are established, this may not always be a conclusion resting on an exhaustive list of alternative conditions. Similar conditions like «joint accommodation» or «joint accommodations as registered in the National Population Register» would probably not have been considered.

3.3 From free-hand rules to law-drafting tools

Traditionally, the process of drafting legislation has been a political process separate from the process of implementation. Since the Sporadic proposals of «automation-friendly legislation» have been advanced since the mid-1970s.[17] In its most extreme version, automation-friendly laws were thought of as hy-

17 See e.g. Jon Bing: Automatiseringsvennlig lovgivning, I: Tidsskrift for rettsvitenskap 1977 (s 195-229).

brids of traditional legal rules and programming statements, considered «brutal» and unacceptable by the legal-political system. Thus, respect for the political process and resistance against technology has absolutely prevented such changes of the legislative process.

In Norway, like in most other countries, there are currently no specialized ICT-tools to support the law-drafting processes. Moreover, only fragments of regulatory methodologies exist, meaning that legislation is by and large drafted «free-hand» with more or less experienced legal expertise.[18] It may be claimed, in other words, that there is a general need to develop law-drafting tools in order to improve the regulatory process. Such tools may first and foremost contribute towards improving legislation expressed in natural language. At the same time law-drafting tools may prepare the ground for formalization and automation - but without representing automation-friendliness in the «brutal» sense mentioned above.

The objective of law-drafting tools should obviously be to improve the quality of legislation. There are various possible requirements regarding regulatory quality which will be too far-fetched to be discussed here. The primary objectives of developing law-drafting tools, however, are to: i) reduce the effort of producing formally correct statutory texts; ii) improve the quality of statutory defined concepts and increase the number of well defined legal concepts and phrases in order to facilitate correct transformation of legal rules to the computer programmes of information systems in eGovernment; iii) avoid definitional differences (of data etc.) which lack political/legal grounds, and compile a library of well-defined legal concepts for the use of law-drafters, system developers and private service providers; iv) strengthen openness and democratic participation in the regulatory process; and v) improve the political control of the regulatory process from political initiative to implementation in information systems.

This represents, to a large extent, a proactive approach because bad drafting causes great and expensive difficulties for government bodies on the level of implementation. For example, if two laws have different definitions of «child support», without any rational reason for this, it will hinder automated exchange of related data and stop redesign of appurtenant routines. Differences based on political and other rational grounds, of course, should always be accepted.

Defined concepts and phrases may gradually accumulate into a library of well-defined concepts which may be used to draft future laws. Provisions

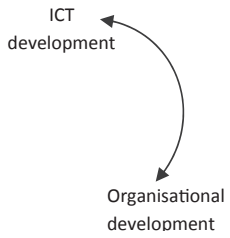
18 See Dag Wiese Schartum: «IT-støtte for arbeid med lovsaker» [Regulatory work and ICT support], CompLex 4/08, Norwegian Research Center for Computers and Law.

regulating access rights to data, for instance, could be expressed with several standardized wordings in natural language, something which facilitates safe transformation to code in eGovernment systems.[19]

4 Reorganization and ICT in eGovernment

4.1 Reorganizing processing of individual decisions

One of the definitions I refer to in section 1 emphasizes that eGovernment is about using ICT in public administration *combined with organizational changes*. These two elements are often interconnected to the degree that it is difficult (and sometimes not possible) to decide which element leads to the other. Here I will not discuss ICT and reorganization of eGovernment as such, but will instead concentrate on some important legal implications of new organizational possibilities and patterns of electronic government.



Core legal issues are linked to the execution of public authority, first and foremost in individual cases, that is, cases where computer programs are developed to automate application of the law. A high degree of automation makes it easier to move tasks from one organization to another, between departments of an organization etc. When the division of labour between man and machine changes and strongly reduces the number of manual operations, it is possible to alter required competence of people carrying out the remaining manual work. This is partly because the number of problem areas is reduced, and partly because it is possible to give sufficient problem-solving support by use of information systems. Most case processing of claims for benefit B has for instance been automated with standardized routines, except hard cases of type B(x) and B(y) which partly are handled by officers in charge. Required expertise by these officers may thus be linked to cases of types x and y, and these officers may receive guidance and support by use of a specially designed legal information system.

19 The NRCCL develop a prototype ICT tool to support the regulatory processes (cf. the project «Regelverkshjelpen» («Regulatory Aid») in collaboration with the Norwegian Ministry of Justice and Police. The idea is to assist the whole process of drafting Acts of Parliament, regulations pursuant to Acts etc.

The organizational flexibility which often follows development of eGovernment systems make it possible to change division of work regarding individual decision-making by government agencies. Firstly, it may facilitate changes within the government sector, for example the transfer of tasks from one agency to another, merger of agencies[20] and establishment of common functions/services for several agencies.[21]

Equally important are possible changes between the government sector and the private business sector. Most important are businesses as potential suppliers of personal data[22] to the government sector, in particular the transfer of data as a basis for individual decisions by government agencies. Employers, banks, insurance companies, etc. are examples of businesses which collect and store personal data required by government agencies in the course of their decision-making. An important eGovernment strategy is thus to establish legal duties for businesses to collect, assure quality and export such data in prescribed machine-readable formats to one or several government agencies. In case, businesses are not formally made part of the machinery of government, but are made part of a government information infrastructure.

The high degree of automation and use of other types of computer support may further prepare the ground for businesses to operate as decision-makers in their own individual cases, without the effect that the relevant government agency loses control to any great extent. One Norwegian county, for instance,[23] has developed an information system for cases regarding grant of free legal advice.[24] Local law firms operate the system in types of cases which are defined by the system as easy, while the county administration decides in complex cases. Another example is the use by private businesses of the decision system adopted by the customs service, which gives access to self-declaration of goods traffic by forwarding agents, etc. Access to the system is conditioned by application to the customs authority, and granted access both creates a right and a duty to use the decision system.[25] It is important to distinguish between information systems like those mentioned here, where private businesses are directly linked to and users of decision-making systems

20 Cf. the merger of the Norwegian (former) National Insurance Administration, Labour Market Administration (both state level) and the Social Security Offices (local level) into Norwegian Labour and Welfare Organisation.

21 Cf. for instance the Internet service Altinn.no, which is a collaboration between 23 government agencies, containing coordinated collection of data from businesses and individuals through a common portal.

22 As well as business data.

23 The county of Sogn og fjordane.

24 Cf. regulation regarding free legal aid of 12 December 2005 nb.1443, chapter 3.

25 Cf. regulation regarding customs of 17 December 2008 nb.1502, section 4-13.

of government administration, and other systems which merely give access to or communicate information.

Businesses that are direct users of government decision-systems for processing cases may be said to use «self-service» facilities, in the sense that they have to do the work themselves. The term «self-service», however, is first and foremost used to describe a division of work were citizens may access information, initiate individual cases regarding themselves and even process their own cases.[26] Self-service government implies in other words that citizens are left alone with their legal and other problems, and try to solve them by means of information and tools made available to them through government Internet sites.

Easy legal problems may be solved even though information and tools are poor, and it may not even be important to identify the question as legal.[27] Hard legal problems will probably not be solved securely in a self-service mode even with advanced information and tools: Information and tools on the Internet offer standard answers and performances, while hard legal problems have no standard solution.

Some would say that no self-service is the best service, and that it should be seen as a blessing for citizens to be «redundant» when individual cases are processed. If a sufficient number of businesses and government agencies could supply government agencies in charge of decision-making with correct information in machine-readable form, decisions could be made automatically without the interference of each individual party in the case. If so, citizens may not even notice the decision-making process itself – only the effects.

I have pointed to some possible organizational models which may be facilitated by ICT. It is important, however, to see that no single model is adopted out of technological necessity and that a wide freedom of choice exists when we design future eGovernment. The different models also have different legal implications, and such possible consequences will of course have an impact on how we create combinations of ICT and organizational models. Here I will only discuss two central legal implications. Individual autonomy and self-control are key words.

26 Cf. St.meld. nr. 17 (2006-2007) Eit informasjonssamfunn for alle [White paper concerning «information society for everybody»), section 7.3.1, action 1.

27 The question as to whether or not one should «support a child under the age of 18 years» is in most cases obvious and does not create any need to check legal sources. A lot of difficult legal questions, however, may arise in the semantic currency grid of such expressions.

4.2 Reorganizing processing of individual cases and the role of parties

During the last fifty years or more, our government sector has been based on the idea that citizens are autonomous and active parties to their own cases. Thus legislation such as the Public Administration Act (PAA), Personal Data Act (PDA) and Freedom of Information Act (FIA) has the protection of legal rights for individuals as its main policy instrument. Right to be notified, access rights, right to be informed and confront the accuser, right to lodge complaints and right to receive grounds for decisions are important examples of legislation based on the active role of parties to cases and other citizens. Self-service government may be seen as a reflection of this approach because the underlying assumption is that of active citizens.

Prevailing self-service eGovernment, however, is not first and foremost about assisting people in the execution of their rights. On the contrary, these types of general legal rules are only to very limited degree made part of eGovernment systems, cf. section 2.2 (above). Self-servicing in existing Norwegian eGovernment systems is primarily about getting citizens to carry out basic administrative work leading up to individual decisions: It is only marginally about reinforcing citizens' abilities to identify and pursue their legal rights.

eGovernment seems in general to overestimate service aspects («we are here for you») while at the same time it underestimates aspects of authority and citizens' possible role of being subjugated («we decide and you obey»).[28] eGovernment is of course not delimited to the «nice» parts of government, and in the not-so-nice parts, possible ICT support for the execution of legal rights would of course be important, but is rarely at the disposal of citizens.

If the goal is to prolong and develop the traditional idea of the legally active and autonomous citizen, future self-service eGovernment should, in other words, have more focus on possibilities of conflicts between government and citizens. In this case, ICT-based information and tools to perform legal rights should be one of the core priority areas.

Self-service eGovernment must, of course, live up to general principles of administrative law, which implies that processing of individual cases must be properly executed (cf. principle pertaining to proper processing of cases). The majority of legislation relating to public administration is comprehensive and complex, entailing that proper, self-service processing of cases is very challenging. ICT solutions of self-service government have to enable citizens to carry out their part of case processing in a legally proper way. Given the complex

28 See, Dag Wiese Schartum: «ICT, service policy and changed division of work between citizens and government. Towards a distributed, user-monitored government?» Electronic communication law review 2002;9(1):7-22.

nature of administrative law, such a requirement would in many cases be difficult and even impossible to live up to.

Requiring proper legal processing of individual cases would make it unacceptable to develop information systems solely relying on citizens to solve hard legal problems alone. Hard legal problems may here, for the sake of simplicity, be defined as i) problems which have direct influence on legal rights and duties and ii) areas associated with justifiable doubt as to how a legal problem should be comprehended and solved. It follows that the question of whether or not a legal problem is hard, relies to a large extent on each individual case. How hard it is to understand a legal provision will depend on how adequate and precise the wording is when compared to the facts of the specific case.[29] This general observation is even true if a party's contribution to a case is very limited: The decision concerning whether or not you «support children under the age of 18», may be hard to make if your teenager is on a trip around the world mainly at her parents expense.[30] Misconception of one detail concerning the understanding of a legal phrase («support children ...») may of course lead to incorrect decisions, even if 95% of the regulation in question is easy to understand.

It follows from the assumption that distinctions between hard and easy cases may be made first and foremost in individual cases, that information systems and other remedies necessary to solve hard problems should be available to any user. Access to individual communication with experts who can help solve individual problems should be included among other remedies. I assume, in other words, that proper legal processing of individual cases entirely based on self-service will be impossible. Realization of legally acceptable self-service decision-making procedures therefore point in the direction of advanced legal information systems at the disposal of citizens. The more citizens such systems are able to support, the less demand for manual assistance there will be.

Advanced legal information systems and possible access to direct expert contact should not only be a requirement in case of self-service solutions. The contrary model, where every piece of information in individual cases is collected from others than the party of the case, and with subsequent automatic case-processing, would probably require similar solutions: ICT may be used to totally exclude parties to cases from the decision-making process, or at least reduce their role to a minimum.[31] In this event, it would mean a shift of

29 Incidents of analogue application of a provision will in other words typically imply a difficult legal problem.

30 However in the great majority of cases the requirement for «child support» is so easy to conclude that it is thought of as a simple factual consideration rather than a legal question.

31 The ICT-based taxation routines of individual taxes are one core example of such a decision-making process.

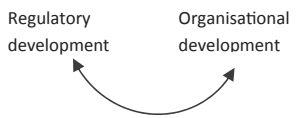
government paradigm. The very concept of constitutional government is built on the idea of basically free and autonomous citizens. Self-determination presupposes involvement and opportunity to act in pursuit of one's own interests. Thus, a government reform which removes such opportunities or dramatically reduces them creates tensions between these basic concepts. The exercise of governmental power in individual cases without significant involvement from the relevant parties is hardly an acceptable model for the division of work in future eGovernment.

The insistence on a role for parties in cases in future eGovernment decision-making processes does not imply that parties' role must remain unchanged. The role of citizens today is largely to carry out preliminary work which previously was handled by officers in charge. Parties to cases could alternatively be involved in review of legality after a decision is reached, or preferably when a *proposed* decision is made available. If so, it is obvious that they need advanced legal information systems which can enable citizens to check legality. Such systems should even support the exercise of statutory legal rights (lodge complaints, receive grounds for decisions etc.). Instead of creating a scene for participation by parties similar to first instance case-processing, it will be possible, in other words, to create a scene similar to a body of appeal.[32]

5 Organizational development and the law

5.1 Exceeding hierarchies

In section 4 I discussed some legal implications of two main models of how ICT and reorganization may be combined. The issue in this section concerns more direct links between reorganization and legal development. Discussions, in other words, are directed towards change processes related to organization and law. These discussions have their origin, to a large extent, in the development of information systems, and electronic government is, in any case, merely a backdrop.



In Norway, organizational power is normally a prerogative of the government. Parliament as legislator, however, may pass bills with organizational

32 A problem of course is that a relatively high number of parties to cases are not able or willing to become involved in the processing and legality control of their cases – regardless of how advanced support information systems are. This is a general problem, however, not only linked to the sketch of a possible redefinition of the role of parties to cases, and may not be an argument against the idea as such.

elements, and history has witnessed acts containing provisions regarding the number and placement of local offices of state agencies. It is also customary that the legislator establishes new government agencies with particular responsibilities. The DPA has, for instance, a statutory basis for the existence of the Data inspectorate.[33]

Main legal regime for organizational powers of government is built on a hierarchical logic, with King in Council at the top,[34] and with ministries, directorates and perhaps local offices of central government as subordinated bodies. Supervisory authorities and ombudsman agencies add to this picture and constitute more or less independent government bodies or bodies placed directly under Parliament. Unwritten rules regarding exercise of powers exists within this organizational framework. Key words are, for instance, rules regarding instruction and delegation, and principles regarding exercise of powers in personnel, procedures and subject matter.

eGovernment in Norway may be partly characterized by a need to overreach and modify existing hierarchal structures. Firstly, current eGovernment efforts are to a large extent geared towards improving interaction and interoperability between the various separate hierarchal lines (typically under different ministries). Interoperability between various branches of government is encouraged and realized through design of inter-organizational information systems, informational infrastructures etc. These types of changes may obviously require modification of hierarchal structures and changes in the use of existing hierarchies. Bodies subordinated under different ministries must, for instance, be capable of establishing common decision-making structures replacing strict hierarchal procedures. Tasks and responsibilities may alternatively shift from one branch of government to another. It follows from the legal understanding of organizational powers that such changes require formal decisions; they are not something management of eGovernment projects can simply do because serviceability is in place.

Developments of eGovernment solutions also create needs to overreach and modify hierarchal structures because government agencies lack technological and other required competencies and capacities required in the change processes. This is in particular evident with regard to technological development, but is probably also true with regard to organizational and regulatory development. To the extent government agencies have competent people; their capacity will nonetheless often be insufficient in situations of comprehensive and complex eGovernment development projects. It follows that the govern-

33 See DPA section 42.
34 I.e. the government as collegiate body.

ment sector frequently has to *outsource* tasks. A government agency with decision-power will, in other words, have to collaborate with private businesses without such powers. Instead of controlling work processes internally by means of delegation, instruction and control, the government agency will have to collaborate and control the process through agreements. In this event, a major legal demand is that the private business (as engaged party) shall not be elevated to the position of *de facto* executor of government decision-making authority. Viewed from the other side, the government agency must (as principal) be in full control of the results of activities of the engaged party to the extent that these activities have impact on decisions in individual cases. The organization of the outsourced work should, in other words, ensure that legal and political responsibilities regarding execution of government powers, remain with the government. Responsible government bodies should be in position to prevent engaged consulting companies from performing erroneous programming that results in incorrect individual government decisions when the system is subsequently put into regular use.

Both mentioned needs of overreaching and modifying hierarchal structures require novel organizational and contractual solutions. Needs may be met project by project, but in my view it is a requirement that a standard toolbox is developed to solve typical problems. As far as I can see, no unbridgeable legal obstacle exists for interoperability and outsourcing in the government field, but legal solutions are currently lacking, insufficient or premature.

5.2 Pushing legal organizational concepts to the limit

Organizational elements are sometimes under statutory regulation, meaning that eGovernment organizational arrangements are bound by legislation. Governments may of course propose amendments to the Parliament, but this procedure is obviously much more cumbersome and time-consuming than situations where basic organizational powers suffice.

Data protection legislation, including information security regulations contains important organizational conditions and requirements. At the core of this legislation is the identification of certain participants and roles each participant must play. The role as «controller» is essential and pursuant to the DPA and appurtenant regulations, each controller should have persons with day-to-day responsibility for fulfilling the obligations of the controller, security management and security audit.[35] This regime does not determine exactly how eGovernment systems should be organized, but establishes certain organizatio-

35 Cf. Data Protection Act section 32 and Personal Data Regulations sections 2-3 and 2-5.

nal frameworks and requirements which must be observed. The bottom-line is that a legally responsible organization must exist and, more importantly, it follows that confusion pertaining to responsibility in the processing of personal data will be deemed illegal.[36]

Although not explicitly expressed in the DPA, the legal regulation of how processing of personal data should be organized provides room for shared responsibility. If several local governments wish to establish common operation of certain personal data, this could be accepted provided the organizational solution does not endanger compliance with the DPA. A great variety of shared controller arrangements are accepted in practice. We may see this as sign of a flexible regulation. The flexibility, however, was not put in place intentionally, but it expresses the situation at the time before the directive was decided (1995) and the subsequent technological development. The normal situation before 1995 was that information systems clearly belonged to one specific organization. Indeed, the Data Protection Directive[37] opens up for a certain collaboration between several controllers (cf. «alone or jointly with others» in the definition of «controller»). However this was only introduced by the European Parliament before the adoption of the Directive.[38] The definition was mainly formulated on the basis of one controller, and collaboration between controllers was expected to be simple and based on equal relations. The many kinds of «pluralistic control» which may exist today were not foreseen.

Today, various architectures of inter-institutional systems and other types of close ICT collaboration between local governments have been much more frequent, and push the definition of «controller» to the limit.[39] Organizational innovation regarding how ICT-systems in government sector should be developed and managed, has pushed the legal regulation of controllers, and made it necessary to admit many other organizational arrangements than original-

36 In the sense that those involved in the processing are obliged to clarify the question.

37 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

38 See Article 29 Data Protection Working Party, 00264/10/EN, WP 169, Opinion 1/2010 on the concepts of «controller» and «processor», adopted 16 February 2010, section III.1.d.

39 The wording of the Norwegian DPA does not contain the alternative «alone or jointly with others». The question is indeed discussed in the preparatory works of the act (Ot.prp. nr. 92 (1998-99) Om lov om behandling av personopplysninger (personopplysningsloven)), but is limited to a situation where a subordinated government agency may be said to act as controller together with a superior authority (e.g. ministry). A commentated edition to the DPA (Wiik Johansen et al, «Personopplysningsloven. Kommentarutgave, Oslo 2001) does not discuss if several controllers may collaborate.

ly thought of.[40] One rather simple legal organizational model has, in other words, dissolved into a great variety of possible organizational patterns. Or as Article 29 Data Protection Working Party expresses it: «a broad variety of typologies for joint control should be considered and their legal consequences assessed, allowing some flexibility in order to cater for the increasing complexity of current data processing reality.»

The described variety of controller constructions makes it very difficult to draft detailed legislation in advance and points in the direction of a changed regulatory strategy. Within eGovernment there are at least two strategies that may be of particular interest. Firstly, eGovernment systems are almost always closely connected to specialized legislation, that is,. it will almost always be possible to place organizational elements of a regulation as part of such legislation, for instance by explicitly deciding how the controller function should be organized. Secondly, and in accordance to recommendation of the Article 29 Data Protection Working Party, the question of controller responsibility could be a matter of agreement, for example between various collaborating government agencies.

Such specific resolutions of organizational questions, established in specialized legislation or/and agreements, are prerequisites for the triangular perspective in the development of eGovernment systems as argued in this article: It is of course impossible to amend the DPA each time various government agencies change the way their processing of personal data is organized. Use of specialized legislation and agreements makes it much easier to consider relevant technological, organizational and juridical aspects in conjunction with one another and regulate accordingly.

6 Conclusion

I have argued in favour of an integrated approach to development of eGovernment systems where development of ICT systems, organizational development and regulatory development are seen as equally necessary and important. The three change processes may not be seen as separate from each other without Government running the risk of seriously deviating from fundamental ideas and principles of our legal system.

A survey from 2009 among lawyers in Norwegian Government administration showed that as many as 55.1 % of the respondents disagreed with a

40 A thorough discussion of «controller» is found in Article 29 Data Protection Working Party, 00264/10/EN, WP 169, Opinion 1/2010 on the concepts of «controller» and «processor», adopted 16 February 2010.

statement saying legal questions related to government use of ICT received sufficient attention. Only 11.4 % agreed. The survey also documented that a clear majority of the respondents confirmed a high number of unsolved basic legal questions within eGovernment.[41]

It is appropriate to ask who should feel responsible for safeguarding legal ideas and principles of our legal system when governments are transformed by ICT? The answer is of course the lawyers themselves. I have argued that a core task is to develop regulations in accordance with the development of information systems and organizations. However, integrated change processes will not become reality merely on the basis of good intentions. Presumably nothing much will happen unless people with primary legal responsibilities adapt to a methodological approach similar to that of computer scientists. The challenge is threefold. First, lawyers must develop adequate methods for the design of logically and linguistically consistent laws, i.e. laws which contain as little ungrounded ambiguity as possible. Ambiguity and discretion should, as far as possible, always be intended from political, juridical or other rational reasons. Secondly, these methods should prepare the ground for communication and collaboration with computer scientists and system designers. Legally based methods should thus probably be developed in conjunction with or inspired by system development methods. Thirdly, ICT tools are needed to support the application of legally grounded methods and to ensure proper safeguarding of legal, technological and organizational aspects.

41 See Dag Wiese Schartum: «Kunnskapsbehov om juridiske spørsmål i elektronisk forvaltning. Resultater fra en spørreundersøkelse blant ansatte i offentlig forvaltning» [Needs for legal knowledge in electronic government. Results from a survey in government administration], Norwegian Research Center for Computers and Law, CompLex 5/10.

HVORDAN MANIPULERE RISIKOVURDERINGER? ERFARINGER OG OBSERVASJONER FRA SKOLESEKTOREN

Tommy Tranvik

Personopplysninger og grunnopplæringen

Skoleeiere i grunn- og videregående opplæring behandler store mengder personopplysninger om ansatte, elever og foreldre/foresatte ved bruk av elektroniske hjelpemidler. Disse hjelpemidlene omfatter blant annet skoleadministrative systemer, digitale læringsplattformer, hjemmesider, e-postsystemer, bærbare eller stasjonære datamaskiner, pedagogisk programvare, sosiale medier og ulike typer pedagogiske nettressurser.

Skolen behandler ikke bare alminnelige personopplysninger om elever, ansatte og foreldre/foresatte. Den behandler også en god del sensitive opplysninger, for eksempel når det gjelder elever med lære- eller atferdsvansker, elever med vedtak om spesialundervisning, elever som av religiøse eller livssynsmessige grunner ikke kan delta i deler av den vanlige undervisningen, elever med vanskelige hjemmeforhold, opplysninger om de ansattes sykefravær og deres fagforeningsvirksomhet.

Skoleeiers elektroniske behandling av både alminnelige og sensitive personopplysninger fører til at personopplysningslovens og personopplysningsforskriftens bestemmelser om informasjonssikkerhet kommer til anvendelse. Disse bestemmelsene innebærer blant annet at skoleeier plikter å sørge for tilfredsstillende informasjonssikkerhet.[1] Det viktigste arbeidsredskapet som skoleeier pålegges å anvende for å oppfylle kravet om tilfredsstillende informasjonssikkerhet, er risikovurderinger. Risikovurderinger skal også anvendes når opplysninger om eller vurderinger av enkeltpersoner (personopplysninger) inngår i manuelle personregistre, for eksempel papirbaserte personal- og elevmapper. Slike vurderinger kan derfor sies å være hjørnesteinen i skoleeiers arbeid med informasjonssikkerhet.

1 Se personopplysningsloven § 13 og personopplysningsforskriften § 2-4.

Hensikten med artikkelen

Hensikten med denne korte artikkelen er imidlertid ikke å diskutere lovverkets krav til risikovurderinger og informasjonssikkerhet. Hensikten er isteden å vise hvordan skoleeier kan gå frem for å påvirke og manipulere gjennomføringen av risikovurderinger. Med påvirkning og manipulering menes at skoleeier anvender metodikken slik at han får det resultatet han ønsker (for eksempel at et IT-system vurderes som sikkerhetsmessig forsvarlig selv om bruken av det kjennetegnes av en rekke alvorlige og kjente sikkerhetssvakheter).

Det betyr at artikkelen handler om (a) hvor sårbare risikovurderinger kan være og (b) hvor enkelt det er å påvirke eller manipulere utfallet av vurderingene. Artikkelen kan derfor forstås som en håndbok i hvordan skoleeier kan gjennomføre risikovurderinger på en slik måte at han får et resultat som bestilt.

Kort om risikovurderinger

Formålet med risikovurderinger er å avdekke, analysere og forebygge hendelser som kan føre til krenkelser av den enkeltes personvern.[2] Slike krenkelser kan oppstå dersom behandlingen av personopplysningene fører til brudd på deres konfidensialitet (opplysningene kommer uvedkommende i hende), integritet (opplysningene endres eller manipuleres av uvedkommende) og tilgjengelighet (opplysningene er ikke å få tak i for de som har tjenestelig behov for å bruke dem). Det betyr at ivaretakelse av konfidensialiteten, integriteten og tilgjengeligheten forstås som avgjørende for at «den digitale skolen» skal kunne sikre den enkeltes rett til personvern.

Personopplysningsloven med forskriften stiller ikke krav til at alle hendelser som kan føre til brudd på personopplysningenes konfidensialitet, integritet og tilgjengelighet skal forebygges. Dette gjelder kun for de hendelsene hvor risikoen for brudd på informasjonssikkerheten (konfidensialiteten, integriteten og tilgjengeligheten) er så høy at den ikke aksepteres av skoleeier. Det kan for eksempel tenkes at skoleeier aksepterer at navn, adresse og telefonnummer til foreldre/foresatte av og til blir gjort kjent for personer uten tilknytning til skolen. Men den samme skoleeieren kan ha nulltoleranse når det gjelder risikoen for ekstern spredning av opplysninger om enkeltelevers lærevansker, hjemmeforhold eller diagnoser. Skoleeier vil derfor ikke benytte knappe ressurser på å forebygge den første typen hendelser, men vil isteden anvende ressursene til å forebygge den andre typen hendelser.

2 Med personvern mener lovverket blant annet den enkeltes personlige integritet, privatlivets fred og tilstrekkelig kvalitet på opplysningene (se personopplysningsloven § 1).

Bruken av risikovurderinger forutsetter at skoleeier har tenkt igjennom hvilke krav som skal stilles til informasjonssikkerheten i skolen: hvilke typer hendelser vurderes å ha såpass liten betydning for personvernet at skoleeier kan godta at det av og til «glipper», og hvilke andre typer hendelser er av en slik karakter at skoleeier ikke under noen omstendigheter kan godta at de inntreffer? Når skoleeier har bestemt dette, har listen blitt lagt for hvor streng informasjonssikkerheten i skolen skal være.[3]

Oppsummert kan vi si at lovgivningen (og Datatilsynets forvaltningspraksis[4]) innebærer at det stilles følgende krav til risikovurderingsprosessen:

1. avdekke hvilke hendelser som kan føre til brudd på personopplysningenes konfidensialitet, integritet og tilgjengelighet,
2. vurdere risikoen forbundet med hver av hendelsene: hvor ofte kan de ulike hendelsene skje (sannsynlighet) og hvor alvorlige krenkelser av personvernet kan de ulike hendelsene innebære (konsekvens),
3. rangere hendelsene i forhold til risiko, for eksempel høy risiko (svært sannsynlig og meget alvorlig), middels risiko (nokså sannsynlig og relativt alvorlig), osv.,
4. iverksette tiltak for å forebygge hendelser med så høy risiko (for krenkelser av personvernet) at skoleeier ikke aksepterer at de inntreffer, og
5. gjennomføre nye risikovurderinger, både jevnlig og ved behov (for eksempel ved innføringen av et nytt IT-system), for å avdekke, analysere og forebygge nye uønskede hendelser (brudd på personopplysningenes konfidensialitet, integritet og tilgjengelighet).

Empiri og metode

Drøftelsene i den første delen nedenfor er basert på empirisk materiale som ble innsamlet gjennom observasjoner av 18 risikovurderinger hos fire skoleeiere i Sør-Norge (risikovurderingene ble gjennomført høsten og vinteren 2010/11). Dette var imidlertid risikovurderinger som ble gjennomført på en meget grundig og profesjonell måte. Den metoden jeg har benyttet for å få frem sårbarhetene ved risikovurderingsmetodikken, er derfor å snu fremgangsmåten som ble benyttet på hodet, det vil si å se på hva som skjer hvis man gjør det motsatte av det som ble gjort i de 18 risikovurderingene.

Drøftelsene i den andre nedenfor er basert på offentlig tilgjengelige dokumenter fra en risikovurdering gjennomført av en større norsk skoleeier (do-

3 Se personopplysningsforskriften § 2-4 3. ledd.

4 Se Datatilsynets veileder i risikovurdering på www.datatilsynet.no/templates/article____888.aspx.

kumentene er hentet fra skoleeierens hjemmeside). Disse dokumentene gir et konkret og reelt eksempel på hvordan en skoleeier har brukt risikovurderinger for å få det resultatet som skoleeieren på forhånd synes å ha bestemt seg for.

Hvordan manipulere risikovurderinger – teoretisk diskusjon

En risikovurderingsprosess består av tre faser: planlegging, gjennomføring og etterarbeid. Innenfor hver av de tre fasene finnes det mange ulike fremgangsmåter som kan benyttes for å manipulere eller påvirke resultatet av vurderingene. Nedenfor gjør jeg rede for de viktigste og enkleste av disse fremgangsmåtene.

Jeg har tatt utgangspunkt i at skoleeier har en interesse i å avdekke, analysere og forebygge så få uønskede hendelser – altså brudd på personopplysningenes konfidensialitet, integritet og tilgjengelighet – som mulig. Skoleeiers bakgrunn for sitt ønske om å manipulere eller påvirke risikovurderingene er derfor å finne så få svakheter og å unngå å bruke penger på nye sikringstiltak. Hvis skoleeiers interesse er det motsatte – å finne så mange svakheter ved informasjonssikkerheten som mulig (for eksempel som et påskudd for å avvikle bruken av et upopulært IT-system) – vil anbefalingene bli noe annerledes.

Prinsippene for manipulering eller påvirkning av risikovurderinger er imidlertid de samme uavhengig av om interessen er å unngå å finne svakheter ved skoleeiers behandling av personopplysninger eller om den er å finne så mange svakheter som mulig. Det bør også understrekes at de manipulerende fremgangsmåtene som drøftes nedenfor ikke bare gjelder når skoleeiere gjennomfører risikovurderinger. De kan også brukes av andre typer virksomheter.

Planleggingen: Denne fasen omfatter to viktige beslutninger. For det første å bestemme hva som skal risikovurderes. For det andre å bestemme hvem som skal delta i risikovurderingen.

Den første avgjørelsen – hva som skal risikovurderes – dreier seg om hvordan risikovurderingen skal dimensjoneres: hvor omfattende skal den være? Skal den kun fokusere på behandlingen av personopplysninger i (eller i tilknytning til) ett av skoleeiers IT-systemer (for eksempel det skoleadministrative systemet eller den digitale læringsplattformen)? Eller skal den også fokusere på flere ulike IT-systemer og alle de arbeidsprosessene som foregår i tilknytning til IT-systemene (for eksempel fraværs- og karakterregistrering eller utarbeidelse av halvårsrapporter for elever med vedtak om spesialundervisning)? Og skal den kanskje også omfatte aspekter som har med fysisk sikkerhet å gjøre (for eksempel hvordan datarommet er sikret)?

For de som ønsker å starte manipuleringen i denne tidlige delen av prosessen, gjelder følgende tommelfingerregel: Jo mer omfattende og ambisiøs risikovurderingen er, desto større er sjansen for at resultatet vil bli slik du øn-

sker. Det man derfor kan gjøre er å bestemme at både det skoleadministrative systemet og den digitale læringsplattformen, i tillegg til alle de arbeidsprosessene som disse systemene anvendes til å utføre, skal risikovurderes i én og samme risikovurdering – systemene og arbeidsprosessene skal altså vurderes i sammenheng. På denne måten sikrer man seg at risikovurderingen blir såpass komplisert og uoversiktlig at det blir vanskelig å avdekke og analysere alle relevante uønskede hendelser. Dermed øker også sannsynligheten for at risikovurderingen vil konkludere med at informasjonssikkerheten allerede er tilfredsstillende (eller at skoleeiers bruk av systemene ikke er heftet med alvorlige mangler eller svakheter), og at det derfor heller ikke er et prekært behov for å iverksette nye, kostbare eller omfattende sikringstiltak.

Det neste man kan gjøre for å forsikre seg om at resultatet blir som man ønsker, er å plukke deltakerne til risikovurderingen med omhu. Deltakernes oppgave i risikovurderingen vil være å avdekke og analysere hendelser som kan føre til brudd på personopplysningenes konfidensialitet, integritet og tilgjengelighet. Det innebærer blant annet at det er deltakerne som avgjør hvor sannsynlig en uønsket hendelse er og hvilke personvernmessige konsekvenser den kan tenkes å få. Det er altså deltakerne som bestemmer om (eller i hvilken grad) det er behov for nye, kostbare eller omfattende sikringstiltak. Det betyr at risikovurderingen og resultatet av den vil avspeile holdningene og kompetansen til deltakerne. Vi kan si at risikovurderingen ikke blir bedre enn de personene som deltar i den.

Her er utgangspunktet at man bare skal plukke deltakere som (a) er positivt innstilt til IT-systemene eller arbeidsprosessene slik de fungerer i skolen i dag, (b) har liten kompetanse på hva informasjonssikkerhet, personvern og risikovurderinger dreier seg om eller (c) begge deler. På denne måten kan man sikre seg at systemene eller arbeidsprosessene enten blir sett på med positive øyne eller blir sett på med øyne som ikke helt vet hva de skal se etter. Uansett er det trolig at risikovurderingen vil konkludere med at dagens informasjonssikkerhet er relativt tilfredsstillende. Det kan også være en fordel å begrense antallet deltakere til et minimum, for eksempel 3-4. For jo færre som deltar i vurderingen, desto mindre er sjansen for at de selv har erfart eller kjenner til eksempler på alvorlige sikkerhetsmangler.

Det man til slutt kan gjøre i denne fasen av arbeidet, er å bestemme at risikovurderingsmøtene skal være av relativt kort varighet, for eksempel én til to timer. Hensikten med dette er å begrense tiden som deltakerne har til debatt og meningsutveksling. På denne måten begrenses anledningen til å avdekke og analysere veldig mange uønskede hendelser.

Gjennomføringen: Et risikovurderingsmøte består som regel av tre deler: (1) innledning (hvor det blant annet gis en kort innføring i hva risikovurderin-

ger er og hva som skal risikovurderes på møtet), (2) identifisering av uønskede hendelser (deltakerne drøfter og kommer frem til sikkerhetsmessige svakheter) og (3) selve risikovurderingen (deltakerne vurderer de uønskede hendelsene i forhold til sannsynlighet og konsekvens).

Den viktigste aktøren i denne fasen av risikovurderingsprosessen, er lederen av risikovurderingsmøtene. Det er lederens oppgave å gi deltakerne en liten innledning til hva som nå skal skje og å styre debattene på møtet. Dette gir lederen stor makt over hvordan møtet vil forløpe – og (ikke minst) over hvilken atmosfære som vil prege debattene på møtet. For at møtelederen skal kunne påvirke eller manipulere resultatet av risikovurderingene, er det flere ting som vil være avgjørende:

1. At møtelederen evner å fremstille seg selv som en ekspert på informasjonssikkerhet, risikovurderinger og personvern. I og med at det sannsynligvis ikke er noen andre av deltakerne som kan påberope seg særlig kompetanse på disse områdene, så vil dette normalt sett ikke by på særlige utfordringer. Alternativt kan møtet ledes av en person som anerkjennes som en kapasitet på «data». Uansett er poenget at møtelederen bør fremstå som en lokal autoritet – en person som vet og kan mer enn de andre deltakerne om det møtet handler om.
2. At møtelederen evner å styre debattene i den retning han ønsker at de skal gå. Møtelederen bør derfor ikke være en tilbaketrukket ordstyrer som fordeler taletiden mellom ivrige og interesserte møtedeltakere. Han bør dominere møtet: det er lederen som er den aktive parten og som gjennom sitt dominerende engasjement passiviserer de øvrige deltakerne. Dette kan møtelederen for eksempel gjøre ved å kaste frem godt forberedte eksempler på uønskede hendelser. På denne måten kan lederen styre diskusjonene i den retning han ønsker, og henlede oppmerksomheten bort fra de områdene som lederen ikke ønsker skal problematiseres og debatteres. I og med at deltakerne er valgt på en spesiell måte (de er enten positive til hvordan systemer og arbeidsprosesser fungerer i dag eller de vet lite om hva informasjonssikkerhet og risikovurderinger handler om) bør ikke dette representere en veldig stor utfordring for en noenlunde dreven møteleder.
3. At møtelederen er i stand til å nøytralisere debatter om uønskede hendelser (sikkerhetssvakheter) som beveger seg inn på følsomme områder (det vil si områder som lederen ikke ønsker fokus på). Her er det flere teknikker som møtelederen kan benytte seg av. Jeg vil kort nevne to av dem: (1) Lederen kan nøytralisere debatter om sikkerhetssvakheter ved å vise til at skoleeier eller skolen har et IT-reglement (eller andre typer interne rutineverk) som er ment å ivareta det problemet som en uventet brysom møtedeltaker reiser. Hvis edeltakeren for eksempel er bekymret for at så mye sensitiv per-

soninformasjon sendes per e-post, kan lederen si at «dette er ikke et problem som vi ikke trenger å diskutere her – skolen har jo allerede en rutine som sier at dette ikke skal gjøres.» Budskapet er altså at problemet ikke er et problem fordi det finnes en husregel som forbyr praksisen (mens deltakerens poeng nettopp er at husregelen ikke fungerer slik som forutsatt). (2) Lederen kan nøytralisere slike debatter ved å vise til at dette problemet uansett vil bli tatt tak i: «Ja, vi kjenner godt til dette og vi vil sende ut en ny informasjon om hva som gjelder for bruk av e-post, så vi trenger ikke å dvele ved dette akkurat nå.» Deretter kan lederen raskt kaste inn et nytt forslag til uønsket hendelse som deltakerne bes om å drøfte.

4. At møtelederen generelt gir inntrykk av at det stort sett står bra til med behandlingen av personopplysninger «her hos oss». Dersom dette fortrøstningsfulle budskapet formidles på begynnelsen av møtet og gjentas like før deltakerne skal vurdere de uønskede hendelsenes sannsynlighet og konsekvens, er det sannsynlig at det vil påvirke deltakerne – de vil trolig sette lavere verdier for sannsynlighet og konsekvens enn hva de ellers ville gjort. Og dersom deltakerne setter lave verdier vil jo konklusjonen bli som bestilt, nemlig at informasjonssikkerheten for det meste er tilfredsstillende.

Etterarbeidet: Den siste fasen av risikovurderingsprosessen består i at møtelederen skriftliggjør resultatet av møtet og foreslår iverksetting av nye sikringstiltak (dersom det skulle vise seg nødvendig). Møtelederen vil derfor utarbeide en liten rapport som blant annet inneholder en beskrivelse av de uønskede hendelsene som ble identifisert og en oppsummering av hvordan deltakerne vurderte hendelsenes sannsynlighet og konsekvens. Rapporten sendes til de relevante beslutningstakerne hos skoleeier, for eksempel rektor, sikkerhetsansvarlig, skolefaglig ansvarlig eller rådmannen (eller en kombinasjon av disse).

Dersom møtelederen har gjort alt riktig så langt (se ovenfor), så er det ikke mye som står igjen for å sikre det ønskede resultatet. Men det kan likevel oppstå uventede utfordringer. Det kan for eksempel skje hvis møtedeltakerne har gitt en bestemt uønsket hendelse overraskende høye verdier på sannsynlighet og konsekvens. Møtelederens oppgave blir da å ufarliggjøre denne hendelsen i risikorapporten. Hendelsen kan for eksempel være at «sensitive personopplysninger kommer uvedkommende i hende fordi passordene til lærernes private konto på filserveren er for lette å gjette». Lederen mener imidlertid at skoleeiers passord-policy er god nok (for eksempel fordi det er han selv som har laget den), og han har ingen intensjon om å foreslå endringer (for eksempel fordi det vil synliggjøre lederens egne feilvurderinger). Det lederen kan gjøre for å ufarliggjøre denne delen av rapporten er å legge inn sin egen kommentar til deltakernes vurdering. Lederen kan for eksempel skrive at «selv om deltakerne

vurderte passord-policyen som risikofylt, er det lite som tyder på at dette faktisk er et problem. Det anbefales derfor at policyen ikke endres.»

Når de ansvarlige beslutningstakere mottar rapporten fra møtelederen, er det lite trolig at de vil stusse på eller stille seg tvilende til konklusjonene. For det første fordi de fleste av dem neppe har kompetanse på informasjonssikkerhet og personvern. For det andre fordi de trolig er tilfredse med at en vurdering faktisk er gjennomført slik som lovverket krever. For det tredje fordi de er godt fornøyde med at rapporten ikke anbefaler utgiftsdrivende tiltak.

Det er verdt å merke seg at risikovurderingsprosessen kan forløpe på tilsvarende måte selv om det ikke er gjort bevisste forsøk på å manipulere konklusjonene. Dette kan like gjerne skje som følge av manglende kompetanse på hva risikovurderinger er og hvordan de kan gjennomføres i praksis. Mine erfaringer fra grunnopplæringen spesielt og kommunesektoren generelt indikerer manglende kompetanse er en langt viktigere årsak enn bevisst manipulering.

Hvordan manipulere risikovurderinger – reelt eksempel

I tillegg til bevisst manipulering og manglende kompetanse, finnes det også andre årsaker til at risikovurderingsprosesser påvirkes slik at resultatene ikke avspeiler sikkerhetsmessige realiteter. Dette synes å være tilfelle i det reelle eksemplet jeg nå kort vil drøfte.

Drøftelsene nedenfor er basert på dokumenter fra en risikovurdering gjennomført hos en større norsk skoleeier (skoleeier A). I hvilken grad de utfordringene som er påpekt ovenfor gjorde seg gjeldende i denne konkrete risikovurderingsprosessen, er vanskelig å si: jeg kjenner ikke detaljene i prosessen. Poenget med dette eksemplet er imidlertid ikke å diskutere selve prosessen, men å vise hvordan risikovurderinger kan påvirkes av utenforliggende hensyn, det vil si (a) hensyn som ikke har noe med selve risikovurderingen å gjøre og (b) hensyn som går ut over de rent sikkerhets- og personvernmessige.

Utgangspunktet er at skoleeier A bestemte seg for å sette ut deler av behandlingen av personopplysninger til en ekstern databehandler (selskap B). Databehandleren – selskap B – er en større internasjonal virksomhet som tilbyr fjerndrift av IT-tjenester over internett, såkalte skytjenester. De tjenestene som skoleeier A bestemte at selskap B skulle fjerndrifte, omfattet blant annet e-post, kalender, tegneprogrammer og samarbeidsverktøy. Her var det derfor snakk om at selskap B ville behandle store mengder personopplysninger på vegne av skoleeieren, og at behandlingen i praksis ville omfatte både alminnelige og sensitive personopplysninger.

Skoleeier A oppga sterke og tungtveiende grunner for sin beslutning om å benytte seg av selskap B sine skytjenester:

- Skoleeieren var i en vanskelig økonomisk situasjon. Fjerndrift av de aktuelle tjenestene ble derfor oppfattet som en måte å spare penger på (kutte skoleeiers IT-kostnader).
- Skoleeierens driftskostnader på enkelte av de tjenestene som skulle settes ut (spesielt e-postsystemet) ble beskrevet som betydelige. Potensialet for økonomiske innsparinger ved fjerndrift ble derfor vurdert som ikke ubetydelig.
- Skoleeieren hevdet at den manglet nødvendig kompetanse til å ivareta IT-behovene i skolesektoren på en god måte. Økt kvalitet på IT-tjenestene til egne brukere ble derfor oppgitt som en viktig grunn til å velge fjerndrift.

Men for å kunne gjøre dette på en lovmessig måte kreves det blant annet at skoleeier A inngår en databehandleravtale med selskap B. Her skal skoleeieren bestemme hva som forventes av sikkerhet hos databehandleren, og databehandleren må forplikte seg til å levere den sikkerheten som skoleeieren forlanger.[5] Samtidig pålegges skoleeier A å risikovurdere behandlingen av personopplysninger før de blir satt ut til selskap B. Dersom risikovurderingen viser at selskap B ikke kan levere den informasjonssikkerheten som skoleeieren forlanger, kan ikke skoleeieren benytte seg av skytjenestene til selskapet uten å bryte sikkerhetsbestemmelsene i personopplysningsloven med forskrift. Spørsmålet er hva skoleeierens risikovurdering konkluderte med?

Ikke overraskende konkluderte skoleeier A med at bruken av skytjenestene til selskap B var godt innenfor de krav som skoleeieren stilte til informasjonssikkerheten. I tillegg konkluderte risikovurderingen med at bruk av skytjenestene ville øke informasjonssikkerheten sammenliknet med alternativet, nemlig at skoleeieren fortsatte å anvende eksisterende og egendriftede IT-tjenester. Fjerndrift ble altså vurdert som bedre for informasjonssikkerheten enn egendrift.

Disse konklusjonene kom skoleeier A frem til på tross av at den manglet detaljerte kunnskaper om hvordan selskap B ville ivareta informasjonssikkerheten til personopplysningene. Skoleeieren hadde i det store og hele nokså lite kunnskap om hva selskap B gjorde for å ivareta personopplysningenes informasjonssikkerhet. Det skoleeieren tross alt visste baserte seg utelukkende på dokumenter som på et overordnet og generelt plan beskrev hvordan selskapet jobbet med informasjonssikkerhet. Men detaljene manglet altså, og selskap B hadde heller ikke forpliktet seg til å levere den sikkerheten som skoleeieren bestemte (rettere sagt, skoleeieren hadde ikke stilt krav til selskapets informasjonssikkerhet). I praksis innebærer dette at det ikke forelå noen gyldig databehandleravtale. Det neste spørsmålet blir derfor: hvordan kunne skoleeieren

5 Se personopplysningsloven § 15 og personopplysningsforskriften § 2-15.

da konkludere med at fjerndrift var en løsning som oppfylte lovgivningens krav om tilfredsstillende informasjonssikkerhet?

Fra skoleeiers risikovurdering og de øvrige dokumentene som er gjort tilgjengelig på skoleeierens hjemmeside, er det mulig å skimte svaret på dette spørsmålet. Følgende scenario fremstår som sannsynlig:

1. Før risikovurderingen ble gjennomført hadde skoleeieren bestemt seg for å benytte seg av skytjenestene til selskap B. Dette fremgår av dokumentene i saken.
2. Denne beslutningen ble «presset frem» av det vi kan kalle for økonomiske imperativer: nødvendigheten av å spare penger og kutte kostnader i en prekær økonomisk situasjon. Også dette fremgår av dokumentene i saken.
3. Konklusjonene i risikovurderingen var derfor gitt før prosessen ble gjennomført. Sett i lys av den økonomiske situasjonen og det faktum at beslutningen om å sette ut driften av IT-tjenestene allerede var fattet, fantes det ikke rom for å komme frem til andre konklusjoner. Dette er en antakelse, men gitt punkt 1 og 2 ovenfor, så fremstår det likevel som sannsynlig.

Det disse tre punktene indikerer er at skoleeier A tilsynelatende har overholdt lovverkets krav om risikovurdering før driften settes ut til en databehandler. Når jeg sier tilsynelatende, så innebærer dette at kravet er overholdt i form snarere enn i innhold: skoleeieren kan legge frem et papir som viser at en risikovurdering er gjort, men innholdet i risikovurderingen er styrt av andre hensyn enn hva den er ment å fokusere på, nemlig informasjonssikkerhet og personvern.

Den grunnleggende årsaken til forskyvningen i fokus – fra informasjonssikkerhet og personvern til økonomiske imperativer – synes å være at risikovurderingen mistet den autonomien vurderingen er avhengig av. Med manglende autonomi menes at risikovurderingen ble en vurdering av skoleeiers økonomiske risiko snarere enn en vurdering av risikoen for krenkelser av personvernet. Dermed fremstår risikovurderingens hovedfunksjon som å hjelpe skoleeier ut av en vanskelig økonomisk knipe fremfor å ivareta brukernes personvern. I så måte tjente risikovurderingen en legitimerende hensikt – den konfirmerte riktigheten av beslutninger fattet på økonomisk grunnlag under dekke av at dette også var bra for informasjonssikkerheten og personvernet.

Avslutning

Denne korte artikkelen har vist at risikovurderinger kan påvirkes og manipuleres på (minst) to måter:

- For det første på mikronivå: ved hjelp av relativt enkle teknikker kan man påvirke utfallet av risikovurderingen ved å manipulere hvert enkeltelement som risikovurderingsprosessen består av.
- For det andre på makronivå: ved at risikovurderingsprosessen mister sin autonomi slik at den ivaretar helt andre hensyn enn informasjonssikkerhet og personvern.

I lys av det som er diskutert i denne artikkelen mener jeg det er verdt å rette et kritisk blikk både mot risikovurderingsmetodikken som sådan og mot måten den anvendes på.

INNOVATION IN ICT-BASED HEALTH CARE PROVISION[1]

Synnøve Thomassen Andersen, Arild Jansen

Abstract

This paper describes a project redesigning psychiatric services for children and adolescents, introducing a new decentralized model into the ordinary structures of health care services in rural areas in Norway by using mobile phone technology. We apply a multilayer and dialectic perspective in the analysis of the innovation process that created the ICT-solution which supports this treatment model. The salient challenges in our case were related to the contradictions between the existing, dominant power structures and the emergent structures in the different layers in the design structures. We argue that as a result of this development process, the new model emerged with a larger potential for creating a new innovation path than would have been the case if it had been linked to the existing structures. The aim of this paper is thus to contribute to the understanding of how user-driven innovation can break with existing power structures through focusing on different layers in the change processes.

Key words

path creation, innovation process, multi-layer dialectics perspective, health care

1 Introduction

The provision of health care services in rural, sparsely populated areas entails a number of challenges, not least in the field of psychiatric care. The use of ICT has become a mantra for providing decentralized health services, and through

1 Originally published in International Journal of Healthcare Information Systems and Informatics, 6(2), 14-27, April-June 2011. Reprinted by permission of the publisher. Correspondence concerning this article should be addresses to Synnøve Thomassen Andersen, Finnmark University College, Follumsvei 31, N-9509 Alta, Norway E-mail: synnovet@hifm.no and Arild Jansen , Section for eGovernment studies, University of Oslo, Pb 6706. St. Olavs plass, N0130 Oslo, Norway, E-mail : arildj@jus.uio.no

the last 15-20 years, substantial efforts have been done to build an ICT infrastructure for telemedicine in the north of Norway. The infrastructure is based to a large extent on broadband networks to be used for traditional computer applications which cannot necessarily support all types of decentralized health services. However, health care is not primarily a matter of technology. Close collaboration with health care providers and between health professionals and patients is essential for achieving better health care. In Norway, as in many other Western countries, we emphasize decentralization and patient empowerment, along with the recognition that future care models must change in order to be economically feasible and sustainable. The mobilization of patients' own resources, as well as family and community resources can contribute significantly to the healing process (Brennan and Safran, 2003; Ball and Lillis, 2001). In particular, patients should be provided with adequate care and support in order to manage their health problems to the greatest extent possible.

This paper reports from the introduction of one such health program in Finnmark[2] based on the Parent Management Training-Oregon (PMT-O) model. This is a treatment and prevention program for families with children displaying antisocial behaviour.[3] An important part of this project has been the development and implementation of an appropriate technical solution based on mobile phones, which can help the care providers as a well as the patients in their communication and information handling routines supporting the treatment. The users were involved to a large extent in this design work. The term «users» in this case means health care workers, team members and «CYP» specialists (clinics for Children- and Youth Psychiatry), as well as parents, adolescents and children. The result has been the development of a new technical solution along with the organizational changes required to support the implementation of the PMT-O treatment model.

The research focus in this paper is the innovation process that has taken place in this developmental work. We draw upon the concept of path creation (see e.g. Garud and Karnøe (2003)) combined with a multi-layered dialectics perspective, developed by Henfridsson et al. (2009) for an explanation of the critical factors that gave rise to this innovation. We thus claim that one cardinal moment in the design process was the decision to break with the existing technical and organizational power structure, and rely instead on the mobile phone infrastructure and services. However, this implied both the need

2 Finnmark is the northernmost and largest county in Norway, although with a population of fewer than 73 000 citizens.

3 PMT-O is based on «social interaction learning theory», developed by Patterson and coworkers at Oregon Social Learning Center. PMT-O is a detailed program designed to improve parenting practices and indirectly reduce antisocial behaviour in the children

to develop a new technical solution, establishment of a new technical support group and implementation of a new health care organization. In this way the project was able to implement the PMT-O model in close cooperation with the users. We claim that a multi-layered dialectics perspective can be fruitful for explaining innovation outside the product development context in which it originally was applied. We thus pose our research question in the following manner: How can a multi-layered dialectics perspective explain innovation processes in ICT-supported health care?

In the remainder of the paper, we first outline the theoretical framework; next, we present the research methodology, followed by analysis and discussions. The last section concludes the paper.

2 Theoretical framework

Traditionally, research on diffusion of ICT innovation has regarded such diffusions as sequential processes unfolding over specific periods of time (see e.g. Attewell 1992; Cooper and Zmud 1990). However, more recent studies of ICT innovations have shown that they need to be understood as network- and socially constructed, and not as occurring in homogenous and stable social ether among autonomous adopters (Damsgaard, Rogaczewski, Lyytinen 1994). One such research current focuses on path-creation activities which influence technology adoption in organizations.

There is an ongoing work in developing new models related to understanding the innovation process with different focus like knowledge, product processes, design, user participation, organizational change, economy etc. One conceptualisation of the innovation process is presented by Miller and Morris (1999), which acknowledges an appreciation of knowledge as part of the process of creating new products and processes. Von Hippel (1994) introduces the term «sticky information» to describe information that is expensive to obtain, transmit and employ in another location than where it originated.

A social interactionist framework is presented by Kaplan (1998) who present a classic diffusion model based on Rogers´ work (Rogers, 1983). Kaplan´s framework is influenced by theoretical models of several factors; organizational change, adoption and use of innovation, user resistance and evaluation of information systems. This perspective may be useful in information system evaluation research that takes account of organizational issues and traditionally economic oriented innovation processes. Similar research related to the innovation process has to be aware the underlying economic importance to organizations so it might be utilized in practice.

We will present a different focus that has made it possible to get more insight in how to organize innovation, new ways of thinking, and new alternative ways to organize design and implement new technical solutions.

2.1 Path dependency and path creation

David (1985) and Arthur (1989) presented the concept path dependence and brought a dynamic systems view to technology innovation studies. Path dependence argues that history is important in understanding how technological innovations are adopted. However, entrepreneurs are embedded in structure from which they attempt to depart. In contrast to path dependence, path creation is seen as a process whereby innovators seek to deviate from existing thinking. Garud and Karnoe (2001) refer to path creation as proactive innovation:

> *In our view, entrepreneurs meaningfully navigate a flow of events even as they constitute them. Rather than exist as passive observers within a stream of events, entrepreneurs are knowledgeable agents with capacity to reflect and act in ways other than those prescribed by existing social rules and taken-for-granted technological artefacts (p.2).*

Path dependence and path creation thus present different perspectives on innovation processes. Henfridsson et al. (2009) points to the reciprocal nature of path creation and path dependencies that are reflected in actors' ongoing enactment of existing structures. In our case, we will illustrate how path dependency was linked to the existing way of providing health services through the telemedicine infrastructure, while path creation originated through the break with that socio-technical structure and thereby developed both an alternative technical platform and a new way of providing health services.

2.2 A Multi-layered and dialectic perspective

Inspired by Henfridsson et al. (2009), we will apply a multi-layered process model for understanding path creation in ICT-based health care service provision. In their paper «Path creation in Digital Innovation, a multi-layered dialectics perspective», they illustrate how an innovation path within a firm consisted of multiple, intertwined layers (op. cit., p 1). Based on Baldwin and Clark (2000) they outlined a three-layered structure model, including the material, cognitive and organizational layers. In their model, the material layer refers to the tangible instantiation of a particular design, the artefact that performs a set of specific functions that create value for its user, which in our

case is the specific technical solution that shall support the provision of health services.

Second, following Henfridsson et al. (2009), designers need to configure design elements in a specific way in order to produce the artefact. The cognitive layer is a logical design of the artefact that represents the mental scheme underpinning the structure and functions of the artefact being designed. For instance, it specifies the hierarchical relationship and interdependences among design elements, which in our case is described by the mobile phone infrastructure and application systems structure as an alternative to the Norwegian Health Network and its support services. The final, upper layer of structure, the organizational layer, specifies activities performed by various designers and their interrelationships, which in our case is comprised by the project organization and its relation to the County Health Authority, and thus partly in opposition to the Regional Telemedicine organization.

Furthermore, in order to explore multi-layered path creation as a process involving human agency, Henfridsson et al. (2009), based on Yoo et al. (2006), adopt a dialectical view of institutional organization. They conceptualize designers in organizations as agents who are situated in contradictory and multiple layers and point out that a dialectic view offers a perspective for understanding the process by which firms break away from the powerful and systematic force of path dependencies. Our multilayered model can be described as in this way:

ORGANIZATIONAL (TASK) STRUCTURE Design Process: activity that creates a design Our case: The existing and the new decision structures
COGNITIVE (DESIGN) STRUCTURE Design: describes an artefact´s structure and functions Our case: The different IT infrastructures and support structures
MATERIAL (ARTEFACT) STRUCTURE The actual artefact that can be seen and used Our case: The alternative IT solutions that were considered in the project

Figure 1. Layers of structure in the design of an artefact (Adapted from Henfridsson et al. 2009)

3 Research setting and method

The empirical base for our study is a three-year study of a project called «Come Here! – ambulant teams and technology» which introduced a new

health program in Finnmark based on the PMT-O model. The research is thus process-oriented as it has observed the actors, their project setting and technical development work over time including the innovation processes in the design of mobile application and organizational changes. Finnmark County, with its scant 73,000 inhabitants is very sparsely populated. Approximately 20 000 persons are under the age of 20, and in 2007, there were 950 children under the age of 18 receiving daily treatment in clinics for children- and youth psychiatry (CYP). Distances are great between communities and most inhabitants also have long distances to travel to get to the nearest hospital or medical expert. The broadband and mobile infrastructure in the county is unevenly distributed; some areas are well covered by both broadband networks and telephone networks, while others are practically without any coverage at all.

The project was established 1 January 2006 following a decision by the County Health Authority to close down the only psychiatric hospital in July 2005. This hospital was to be replaced by a decentralized treatment model, where ambulant teams would conduct and support home-based treatment for both families and children (between the ages of 6 and 12). The aim was to develop and implement technical solution to support this new decentralized care model with the goal of providing children and families help and treatment wherever they lived, and while taking into account their cultural background, language etc. When the project started, two important decisions had to be made: i) the choice of an adequate professional method and ii) the selection of an appropriate technical platform.

3.1 The professional treatment model

The professional ambulant team decided to use the treatment method based on the PMT-O model, which is an outpatient treatment model for parents with children that can be difficult to raise. The method aims at training parents to cope with and raise their child in better ways. During the initial meeting the team, parents and the child defined and prioritized the goals to be reached. Furthermore, they negotiated the specific patient behaviour that should be encouraged or discouraged through the system (for instance their behaviour during meals or when going to bed). The child's rewards in relation to these action points are defined, as well as how many score points would reward certain types of behaviour. Based on this information, a report is created. The parents, in cooperation with the child, are supposed to register the behaviour and assign a score (between zero and five points) frequently, that is, during every meal, or every evening when the children went to bed. These reports are

the basis for the interaction between the family and the CYP team. Between the visits by the ambulant team, the parents should register the behaviour.

When this model was implemented, some parents would fax the forms to the team, but others kept it until the next time they interacted with the team. It was felt that this collaboration would benefit from more frequent reporting as well as enable easier and more frequent interaction. The project aimed at changing these communication patterns by introducing technology and design that allowed parents to report on and register behaviour immediately, enabling the CYP team to monitor progress on an ongoing basis. Figure 2 shows the organization before the start of the reorganization and project.

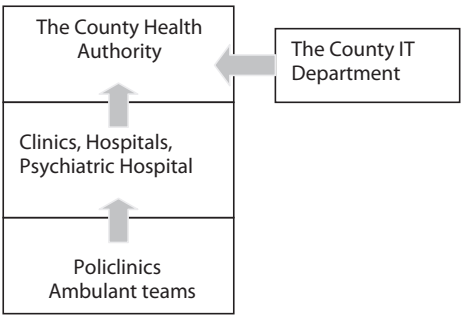


Figure 2. The organization before the project started in 2006

The County IT Department formally withdrew from the project in January 2007, nearly a year after the project started. The grounds for withdrawal were the reorganization of the department as of 1 January 2006 and its integration into the Northern Norway Regional Health Authority (RHF). During this reorganization, the IT divisions in three county health authorities were centralized into one Regional IT Department. It then became more difficult to collaborate with them. Despite multiple enquiries addressed to the County IT Department, the project team never received any documentation of the existing information infrastructure, which is a national broadband network connecting all health institutions. Such information was essential for the progress of the project.

Figure 3 shows the project organization; the steering and project group was formally subordinate to the RHF. The *reference group* and the *techno group* were mandated by the steering group, while the regional IT Department was part of the County Health Authority responsible for technical support and services. The telemedicine organization was represented by this IT Department. The red mark in figure 3 illustrates the conflict between the County Health

Authority and the associated steering group and the Regional IT department, which in the end resulted in a break related both to funding and design of the (technical) system.

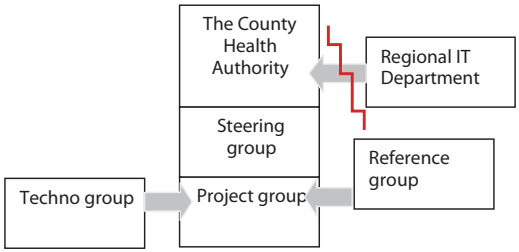


Figure 3. Project organization

3.2 Data collection and analysis

We have used a qualitative research approach in the interpretive tradition of IS research (Myers, 1997: Myers and Avison, 2002; Walsham, 1993). The data collection followed the progress of the project, as one of the authors has been the project manager in this project since the start in 2006. In this capacity she has been directly involved in the developmental work and has participated in multiple project activities. Her involvement has alternated between observation as a participant and active involvement, representing a relatively high degree of engagement, which in turn implies challenges in balancing research interests with the practical needs of the project.

There may be divergent interests between the roles of researcher and agent for change, and it may be difficult to be fundamentally critical if one believes in and champions the project's aims. Walsham (2006) claims that there is a risk for the researcher of becoming «socialized to the views of the people in the field and thus lose the benefit of a fresh outlook on the situation» (op. cit., p. 322). We have tried to avoid the latter by keeping an objective distance from the families/patients. All contact with families has been through therapists in the ambulant teams, and as researchers we have had an open discussion concerning our involvement.

A significant source of data is from the formal meetings, since we have participated in more than 63 meetings. Data has been collected through questionnaires completed anonymously by the families, through interviews with every member of the ambulant teams and interviews with user representatives, through observation of the work in the techno group and, lastly, through qu-

estionnaires completed by members in the project group, steering group, and children from one of the pilot communities. Interviews have been conducted primarily with health care workers in the ambulant team and user groups representing the children and families. All interviews have been transcribed.3 Participant observation is another important source of data, especially through user courses. The study also includes analysis of significant amounts of archival data including meeting notes, workshop documentation, user-training notes, e-mail correspondence and reports. Table 1 shows the data collection activities; the collection technique, type of activities and the total number of data sets. All data sets are interrelated and have been applied in the analysis.

Methods	Type of activities				Totally
	2006	2007	2008		
Observation (during participation in meetings)	3 project team 7 steering group	7 project team 3 steering group 5 contractor	4 project team 3 steering group 5 techno group	other meetings	63
Observation (during user courses)			3 observations		3
Interview	12 from CYP staff	4 user representatives			16
Questionnaire			2 questionnaire		2
Literature	project documents	meeting notes e-mail and reports	user-training notes, workshop documentation	other documents	< 100

Table 1 Data collections methods used

The data collection has been an iterative process, including three, partially overlapping phases: i) planning and analysis, ii) design and experimentation with pilot versions and iii) implementation. The first phase lasted for nearly a year. The discussions and decisions from the meetings were documented by the researcher/project leader through extensive note-taking, for example when planning the design. The participants were aware of the research plans, and did not appear uncomfortable by the note-taking. The notes were then copied, shared and discussed with the administrative participants, the project team and techno-group. Our notes have been read and accepted; only two revisions have been made. Combined with the analysis of relevant literature, this phase

guided the remaining data collection processes. This initial phase is described in more detail by Andersen and Aanestad (2008).

The next phase included design and testing pilot versions; the data collection mainly included observation, workshops and transcribed interviews based on templates from the techno-group, project group and user groups representing the children and families. A total of ten interviews were conducted, lasting between 30 minutes and one hour each. All interviews were based on an interview template developed on the basis of the themes identified in the first phase and especially the responses from the project group. Respondents ranged from user (therapist, health care workers from ambulant teams, representative from the user organization Mental Health Norway and the parents) to developers and thus included expertise in areas such as design and graphical interfaces (related to the method used in the CYP), mobile software development and architecture. Workshops were organized with the project team, the techno group, the reference group, children and the system developers during the last two phases in order to provide feedback and new perspectives on their work practice based on the prototype of mobile application and empirical findings, particularly as related to the design of the application. Discussions between the project group and the techno group resulted in the conclusion that technical solutions for psychiatric healthcare must be designed for a specific workplace setting. In these more specialized applications, the user participants in the design work had to take into account the specific effects that the solution may have on the people who will inhabit it. In order to facilitate such discussions, user scenarios (such as *use cases*) were developed by the contractor. A possible conflict of interest was related to the fact that some participants in the project group consciously drew on their background of shared experience in the community and culture, especially since some users had Sámi background. Approximately 40% of the inhabitants in the county are ethnic Samis, a fact which entails challenges related to language and culture.

The application that supports the PMT-O model was developed with user participation and_implemented on mobile phones. The application was distributed to project participants, and the user interface resembles the paper forms used to register the results of specific action points regarding the child's problems. The application is general and adaptable in order to give every child and family the possibility for adapting it to the individual case management plans. The data are sent from the phone (e.g. a list of scores or report on behaviour during meal time is transmitted over the mobile phone network). The CYP workers have access to the information from the server through Internet and VPN- channels. As this is outside the secure health-care network, there is no direct import into the main patient record application, but it is pos-

sible to cut and paste information from the application into the «CYP Data», which is the main patient record application in use in the health care sector.

3.3 Conflicts and contradictions in the design work

A key factor in a dialectic perspective is the potential for contradiction. In our case this became apparent when the project had to decide upon the technical platform. The arguments related to the choice of a decentralized model in favour of the alternative use of mobile telephones were cost considerations, concerns about usefulness as well as technical aspects. The recommendation from the IT Department (ancillary to the National Health Network) was to apply a solution based on videoconferencing including PCs, web cameras, document cameras, etc. This would be considerably expensive, however, compared to the cost of purchasing mobile phones. Videoconferencing technology might also require costly upgrades of the different studios in the out-patient clinics. Not least, since the ambulant teams would be travelling a lot, mobile phones would therefore be more practical for interpersonal communication than portable PCs. Furthermore, the extension of the broadband network in the northern part of Norway is not as good as the coverage of the mobile network. Lastly the training required for children, families and ambulant teams in order to use the videoconferencing solution would be considerable, while the use of mobile phones is widespread in all age groups and social strata of the population.

In January 2008, County Health Authority decided that all communication related to ICT-matters should be handled by one specific office in the administration. For example, enquiries related to the cost of participation from the Regional IT-Department in the project, raised the following question:

> *We need a decision about who is going to pay for the costs involving the Regional IT-Department in the project?*

One week later, the clinic leader responded in an e-mail:

> *There is no money in the project to cover support from the Regional IT-Department. I think that the best solution now is to give the Regional IT-Department a detailed system description from the contractor as a basis for the Regional IT-Department to give us a cost estimate. We will develop a solution based on this.*

However, the Regional IT-Department never responded to this enquiry.

One of the user representatives describes the contradictions as follows:

Due to the IT-Department's absence, the testing and debugging started too late.....You would think that leaders at higher levels have a larger influence on what takes place in that part of the organization, but the reality is that it does not work. This is perceived as rather astonishing.

The last phase was the implementation of the solution, including meetings, user-training, interview and structured questionnaires addressed to future users, and a prototype of the web-based solution was developed. This design work demanded user participation. One of the user representatives describes the work as follows:

The user participation has been strong all the way – at all levels! I had good contact with the project leader in the planning of user courses. I'm experiencing that the user side has had several opportunities to influence and make contact with the project leader.

The design for the prototype was discussed with the different user groups in order to verify and extend the preliminary understanding of the use of mobile phone as a tool for treatment. One of the project team members described this situation as follows:

It has been kind of unclear who owns the project - not on the part of the co- workers in the project, but on the part of management. I think that the leader in the steering group could have been more supporting… It kind of shows a lack of knowledge on how to run a project and on who has the responsibility for what.

Three classes in user training were conducted to test the solution before the model was tested in the project. The contractor had the responsibility for implementing the mobile application. It was important for the techno group to cooperate and work together to design the application based on a variant of PMT-O model. Two of the team members described the test period as follows:

We also think that one should have the opportunity to alter the forms so that the project could be used by others with other sets of problems as well, but what about the IT Department and the County Health Authority – would they be able to come to an agreement?

User representatives in the project group said, on the subject of participation in the project:

I think that, as a user representative, I have been heard. And to a degree it has been possible to bring something into the project. There are examples related to many issues in the project, such as user interface on the mobile phone, content in some of the meetings and so on. For user representatives in general and for me especially, we need experience in the area of contributing as user representatives, and my participation in the «KOM HIT» project has given me a useful experience in my coming work as a user representative.

Another user claimed:

It is very important that all co-workers in a project have a sense of ownership in the projects they are working on. I have the impression that there has been a lack of this at times; that some of those who have been in on the project from time to time haven't had this necessary «ownership». My understanding is that the KOM HIT project has been a very important project from the user-perspective, and historically a path-breaking project. There are several reasons for my incidental comment about County Health Authority's lack of ownership in the project. I believe it is important that County Health Authority will look at this in their internal evaluation – with regards to future projects.

Several representatives in the teams have expressed that a user focus has been important in the engagement, interaction and participation. It resulted in early help and treatment for the families in their own community, and at the same time the families had the possibility to participate and cooperate with the ambulant team in their own treatment. This user focus is described in more detail by Andersen and Van der Velden (2010).

4 Analysis and discussion

The technical solution (called *Come Here – Mobile)*, as illustrated in figure 4 below shall provide access to an information base on a common server and thereby support all user groups. The system has three actors: 1) the families (children and parents), which have access only by mobile phones, 2) the therapists (ambulant team) which have access both through the PC and Internet and by mobile phones and 3) administrators, which also have access both ways. The solution thus uses both the mobile phone network for communication with the patients and the broadband network to support the therapist.

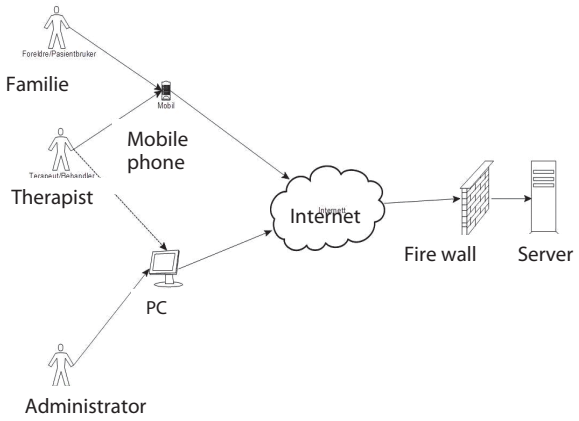


Figure 4. The schematic description of the technical solution

In terms of the multilayered model, we can describe the different activities related to teach layer in the following way.

4.1 Material layer

The technical artefact in our case is the specific solution that shall support the provision of psychiatric health services, based on the PTM-O model. The focus in the material layer is thus on the shift in technical solution and the usability of a videoconference system versus the use of mobile phones. From the end-user's point of view, the artefact comprises both an application on a mobile phone and PC running tailored applications. Before the project was established, the health authority contacted the Norwegian Centre for Telemedicine (NST) for advice on the choice of the technical platform for the project. NST proposed the use of videoconferencing technology and PC-based technology on the existing broadband infrastructure. However, realizing the fact that a technical solution based on mobile phone would have moderate costs and that it would be more user friendly, the steering group and the project team felt that mobile technology based on 3G was the only feasible choice.

4.2 Cognitive layer

The cognitive (design) layer of structure is related to the structure and the functions of the chosen technology and the specific design solutions, which our

case is comprised by the mobile phone infrastructure and tailored applications, as an alternative to the Norwegian Health Network and its support services. The selected solution will thus not be integrated into the national network, but exist as a stand-alone system outside this network. The implication is thus that both the operational capabilities of this solution and the support functions are separated from the health services provided by the Regional Health Authority.

4.3 Organizational layer

The organizational layer of structure specifies activities performed by various designers and their interrelationships. In our case it comprises the project organization and its link to the «local» County Health Authority, and also its problematic relationship to the Regional Health Authority, including the latter's «opposition» to the Telemedicine organization. The County Health Authority which has overall responsibility and control, decided in October 2010 whether this model is to become the permanent standard for psychiatric care for children and adolescents in Finnmark.

4.4 Dominant and Emergent Structure in the Layers

The dominant structure at the existing cognitive (design) layer was the broadband infrastructure supporting videoconferencing technology, which was under the health authority control, while the emergent structure at this layer was based on the 3G mobile technology. In the old structure the IT Department was reorganized in 2006 in the Regional Health Authority. The contradictions in the material (artefact) layer were related to the differences between mobile phone application and the use of videoconferencing technology on PCs, which is also an integral part of the Norwegian Health Network. These aspects influenced the transformation processes across different layers. The «Come Here!» project had to resolve the contradictions at the organizational layer. The adoption of user-driven design method through prototyping, which underlines the differences in the development approach as compared to the standard that Norwegian Health Network was supposed to support. In light of the cognitive layer disappointments, the actors directed their attention to the organizational layer, and in particular County Health Authority, to resolve the conflict with the dominant structure, which was the telemedicine information infrastructure and IT Department.

The IT Department, as a part of The Norwegian Health Network, with contracts to connect all health institutions via a secure broadband network, thus opposed this new technical platform. The decision to use mobile tech-

nology was followed by an unexpected reluctance from the IT Department. This situation resulted in the project's standing «alone» in designing the specific solution, and this had important consequences. On the one hand, it allowed for a lot of flexibility for adopting users' wishes and needs in terms of communication patterns and functionality. On the other hand, the project also emphasized building a flexible solution due to the lack of information about the existing technical infrastructure. A new support function (the techno group, see figure 3) had to be established along with an expansion of the existing mobile infrastructure to include a flexible user interface (the emerging structure). This caused a shift of the innovation path from a traditional top-down development model to a new, partly user-driven bottom-up model. This flexible solution would make psychiatric treatment more convenient, as compared to traditional treatment methods, but this new design effort created contradictions to the existing logic of the closed modular design approach in the healthcare network.

At the organizational (task) layer, the dominant structure comprised a rather centralized organization with regards to decision structure. This was related to the old project organization. In the new organization, the project was anchored in the top level management of the County Health Authority. This structure offered the possibilities to develop and implement suitable technologies to support this new decentralized care model where ambulant teams would conduct and support home-based treatment for both families and children. This situation leads to an emergent structure: a decentralized model that includes both the mobile actors (user groups, techno, steering and project group) participating and contribution in the project, but also the practical usage mode in the different communities. The project group then established the techno group, who developed the new mobile model. This solution entailed a move away from the old structure representing the traditional way of implementing telemedicine, and also the channel for implementation, since the model would be outside the secure health-care network. The contradictions between the dominant and emergent structures are thus related to control of routines and procedures. The project's close link to the County Health Authority also implied that necessary changes related to administrative routines could be more easily accomplished. These changes were not trivial and were related to defining new contract types, new models for purchase agreements and new types of service models (from centralized to decentralized). The type of telephone subscription schemes and reimbursement models were discussed.

We may illustrate our findings related to the three layers of structure in this way:

	Dominant structure	Emergent structure
Organizational (Task) layer	Centralized development model Telemedicine organization	Decentralized development model County Health Authority & techno group
Cognitive (Design) layer	Broadband infrastructure integrated with National Health Network	3G Mobile phone infrastructure and stand alone solution
Artefact layer (material)	Videoconferencing by use of PC	Mobile phone application

Table 2. Structures in the model. Adopted from Henfridsson et al. (2009)

The contradictions within each layer were important resources in the path-creating process. Our research shows that a multi-layered dialectics perspective can be fruitful in explaining adoption of user innovation outside the product development context. The flexible mobile solution included a new application in the design layer. The contradictions between the dominant and emergent structures in the organization layer transformed contradictions into a new negotiated organizational structure. The actors, as path creators, played an active role in building the new organization for psychiatric health care, which illustrates that new innovation paths are never created in a vacuum or isolated from already existing socio-technical arrangements, thus in line with Hanseth (2000). The active role of users as designers also involved critical reflection through participation in the design processes. The work in the techno group, including the involvement of the various user groups, demonstrates how contradictions across structural layers caused the members to be reflective, similarly to what Seo and Creed (2002) describe when users are transformed from passive participants in the reproduction of the existing socio-technical order into active agents of change.

Our analysis illustrates how path dependency at the outset was linked to the existing way of providing health services through the telemedicine infrastructure, while a new path creation process originated through the break with that socio-technical structure. In this way our path creation process developed both an alternative technical platform as well as a new way of providing health services. Our findings seem to be in line with Henfridsson et al. (2009), who claim that the reciprocal nature of path creation and path dependency is reflected in actors' ongoing enactment of existing structures.

5 Concluding remarks

The aim of this paper has been to examine innovation processes, and our analysis addresses more specific the challenge of overcoming existing thinking (path dependency), and thereby trigger of new thinking (path creation). The creation of a new technical and organizational path was made possible through a better understanding of the contradictions that existed. We have applied a research framework that has been developed for a product development environment, but which seems relevant for other research areas, too. Our contribution is thus to help understanding how new innovations may be introduced in existing organizations. The health sector faces huge challenges related the implementation of new technical solutions that require changing organizational structures and work practices. One important clue can be to unveil existing contradictions and dialectic views, in particular related to existing task structures. The case we analysed dealt with how to apply new, mobile technology in service provision in psychiatric treatment. We do believe that our findings are relevant for introducing new technology in other types of health services, and that it in this way may contribute to a better understanding of how to change organizational structures by addressing the different layers of structures in the design process. It is important to get more insight into how to stimulate innovative thinking in the design of new technical and organizational solutions to be used in the health sector.

In our analysis, we explore the contradictions that existed between the previous and emerging organization of health care service provision, and in particular the tensions between different ICT platforms and their support infrastructure. Our research has addressed the question of how to break with the fundamental isomorphism between task structure and design structure. We have found that this multi-layered path creation perspective may help in understanding the innovation processes leading to the development of a new technical solution, and corresponding organizational change processes in health care provision.

The limitations of our study are that it included just one specific case, the introduction of mobile technology in psychiatric treatment. Our findings can accordingly not be generalized without reservations, but it shows at least the relevance of our research framework. However, our finding should be tested in other search settings. More research is thus needed in order to illustrate how this framework may be relevant in other fields in the health sector, and furthermore, to what extent it may offer a conceptual thinking related to changing larger organizations. This type of research is transcending the disciplinary boundaries in that it examines the relationship between organizational design and «product» (artefact) design and illustrates the fruitfulness of a multidisciplinary approach.

References

Andersen S.T. & and Van der Velden, M. (2010): *Mobile phone-based healthcare delivery in a Sami area: Reflections on technology and culture.* CATAc International Conference; 2010, 2010-06-15 - 2010-06. ISBN 978-0-86905-966-1.

Andersen, S. T.& Aanestad M. (2008): *Possibilities and challenges of transition to ambulant health service delivery with ICT support in psychiatry*. IFIP TC8 WG8.2 International Working Conference;2008,2008-08-10 - 2008-08-13. ISBN 978-0-387-09767-1.

Arthur, W.B. (1989): «Competing Technologies: Increasing Returns, and Lock-In by Historical Events. «Economic Journal» (394): 116-131.

Attewell, P. (1992): *Technology diffusion and organizational learning: The case of business computing*, Organizational Science Vol 3. No 1, Feb. 1992.

Baldwin, C.Y. & Clark, K.B. (2000): *Design Rules - The Power of Modularity*. MIT Press, Cambridge, MA.

Ball M.J & Lillis J. (2001): E-health: transforming the physician/patient relationship. *International Journal of Medical Informatics*, vol. 61, no. 1, pp. 1-10

Benson, J.K. (1977): Organizations: A Dialectical View. *Administrative Science Quarterly* 22(1) 1-21.

Brennan, P. & Safran, C. (2003): Report of conference track 3: patient empowerment. International Journal of Medical Informatics 69: 301-304.

Cooper, R. B. & Zmud R.W (1990): Information Technology Implementation research: A technological Diffusion Perspective. Management Science, Vol. 3, No. 1, pp 60-95

Damsgaard, J., Rogaczewski, A. &. Lyytinen, K (1994): How Information Technologies Penetrate Organisations. An Analysis of Four Alternative Models. I Levine (red.) *Diffusion, transfer and Implementation of Information Technology* North Holland, 1994.

David, P.(1985): Clio and the Economics of QWERTY. Economic History, 75, 227-332.

Garud, R., & Karnøe, P. (2001): Path Creation as a Process of Mindful Deviation. R. Garud, P. Karnøe, eds. *Path Dependence and Creation*. Lawrence Erlbaum Associates, Mahwah, New Jersey, 1-38.

Garud, R.& Karnøe, P. (2003): Bricolage versus Breakthrough: Distributed and Embedded Agency in Technology Entrepreneurship. *Research Policy* 32(2) 277-300.

Hanseth, O. (2000): The Economics of Standards. C. Ciborra, K. Braa, A. Cordella, B. Dahlbom, Failla, O. Hanseth, V. Hespø, J. Ljungberg, E. Monteiro, K.A. Simon, eds. *From Control to Drift - The Dynamics of Corporate Information Infrastructures*. Oxford University Press, Oxford, 56-70.

Henfridsson, O., Yoo, Y. & Svahn, F.(2009): Path Creation in Digital Innovation: A Multi-Layered Dialectics Perspective. Sprout Working papers on Information Systems, ISSN 1535-6078. URL: http://sprouts.aisnet.org/9-20.

Kaplan, B.(1998): SocialInteractionist Framework for Information Systems Studies: The 4Cs *IFIPWG8.2&WG8.6 Joint Working Conference on Information Systems: Current Issues and Future Changes*, eds. Larson T.J., Levine, L.&DeGross, J.I.International Federation for Information-Processing.

Miller, W.,L & Morris, L.(1999): Fourth Generation R & D: Managing Knowledge, Technology and Innovation, John Wiley & Sons, Inc., Canada, 1999.

Myers, M., (1997): 'Qualitative Research in Information Systems', MISQ Discovery, 2

Myers, M.. & Avison, D.(Eds.) (2002):. Qualitative Research in Information Systems. London: Sage, 312 pages, ISBN 0 7619 6632 3.

Seo, M.-G.,&. Creed,W.E.D (2002): Institutional Contradictions, Praxis, and Institutional Change: A Dialectical Perspective. *Academy of Management Review* 27(2) 222-247.

Von Hippel, E (1994): Sticky Information and the Locus of Problem Solving: Implications for Innovation,Management Science, Vol. 40, No. 4, 429-439.

Walsham, G. (1993): Interpreting Information Systems in Organizations, Wiley, Chichester, 1993.Walsham, G. 2006. Doing Interpretive Research. *European Journal of Information Systems* 15(3) 320-330.

Yoo, Y., Boland, R.J. & Lyytinen, K. (2006): From Organization Design to Organization Designing. *Organization Science* 17(2) 215-229.

IGOV2: EXPANSION OF gTLD NAMES – AN EVALUATION OF THE OBJECTION-BASED DISPUTE RESOLUTION SYSTEM PROVIDED FOR IN MODULE 3 OF THE APPLICANT GUIDEBOOK.

Kevin McGillivray

Abstract

Creating increased competition in the Internet domain namespace has been a long-time goal of the Internet Corporation for Assigned Names and Numbers (ICANN). After much discussion, planning, and conflict, ICANN is in the final stages of allowing large numbers of new generic-Top-Level-Domain (gTLD) names on the Internet. The goal of the expansion is to foster competition, allow for innovation, and increase consumer choice. ICANN has provided the blueprint for the new gTLD name application process in the gTLD Applicant Guidebook («AG»). The AG provides application guidelines, timetables, and clarifies much of the delegation process. Among other systems designed to protect parties and limit risks to users, the AG provides procedures or systems for resolving disputes. In an attempt at effective dispute resolution, the AG provides for both *ex ante* and *ex post* procedures for challenging the use of new gTLDs.

In this paper, I focus largely on the rights of parties to challenge new gTLD names during the application process. More specifically, this paper focuses on the dispute resolution system in module 3 of the AG. The paper evaluates both the practical steps for objecting to a new gTLD and challenges in application of the procedure. As a point of comparison, the Uniform Dispute Resolution Policy (UDRP) is discussed.

1 Introduction

After much discussion, planning, and conflict, the Internet Corporation for Assigned Names and Numbers (ICANN) is in the final stages of implementing a program that has the potential to greatly expand domain name offerings on the Internet. ICANN's goals of increasing competition, fostering innovation, and providing users with greater choice are some of the central reasons for making available new generic-Top-Level-Domain (gTLD) names.[1] Securing a new gTLD will require an extensive application process and considerable capital. The process and requirements are provided for in the Applicant Guidebook (AG). The AG has evolved through multiple versions and the ICANN board adopted a final version, albeit subject to changes, at the ICANN meeting in Singapore on June 20, 2011.[2]

The AG provides guidelines for applicants, estimates of costs, and clarification of much of the delegation process. Among other systems designed to protect parties and limit risks to users, the AG provides a system for resolving disputes. In an attempt at effective dispute resolution, the AG provides for both *ex ante* and *ex post* procedures for challenging new gTLDs as applied for and as used. In this paper, I focus largely on the rights of parties to challenge new gTLDs during the application process, which occurs prior to delegation or «launch» of a new gTLD. More specifically, I analyze module 3 of the AG, which contains the objection-based system for dispute resolution.

In the second chapter, I consider the module 3 dispute resolution procedures (DRP) provided for in the AG, and consider its application as a form of dispute resolution.[3] I provide some comparison between module 3 DRP, and the more established Uniform Dispute Resolution Policy (UDRP). Procedural and substantive aspects of the new policy will be discussed.

The goal of this paper is two-fold. First, it is to provide a practical analysis of the dispute or conflict resolution systems provided for in module 3 of the AG. This includes some discussion of both historical and current policy debates surrounding the process. Second, it is to consider whether the dispute resolution systems comport with notions of fairness or justice. In the latter respect, I largely consider whether the standards provided for are fair to trademark owners, gTLD operators, and other parties with a stake in new gTLDs.

---

1 «In a world with over 1.6 billion Internet users – and growing – diversity, choice and competition are essential to the continued success and reach of the global network.» Available at: http://www.icann.org/en/topics/new-gtld-program.htm (Last visited May 16, 2011).

2 Available at: http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf.

3 Kaufmann-Kohler, Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice*, page 6 (2004) (Discussing various types of dispute resolution procedures offered online).

This assessment occurs largely through an evaluation of the DRP design and consideration of issues in application of the policy.

1.1 Background: The Domain Name System (DNS)

On the Internet, computers find each other using a string of numbers known as an IP (Internet Protocol) address.[4] The Domain Name System (DNS) operates based on a hierarchy of names and acts as a central system for routing traffic on the Internet.[5] The DNS is not a singular file, but is made up multiple networks. [6] The DNS provides unique IP addresses, which identify individual computers, with domain names.[7] IP addresses are essential to routing packets of data over the Internet.[8] Domain names are not essential for routing packets of data, but are useful as a means of finding other computers on the Internet. By typing a domain name into a browser, an Internet user is able to locate websites with words or phrases instead of numbers. Although domain names are not essential for finding locations on the Internet, they do provide for a more user-friendly method of navigation.[9] For example, to access the search engine Yahoo® an Internet user has the option of entering either <209.191.122.70> or <www.yahoo.com>.[10] The well-worn, but useful analogy is that the DNS system operates as the Internet's phonebook. Internet users can find the IP address they need simply by locating the corresponding domain name. This is similar to finding a phone number by looking up a name.

Domain names are generally read from left to right. Domain names are labeled as being at the Top-Level-Domain (TLD), or Second-Level-Domain

4 Bygrave and Bing, Internet Governance: Infrastructure and Institutions, at 150 (Oxford University Press 2009).

5 Alikhan, Shahid and Mashelkar, Raghunath. Intellectual Property and Competitive Strategies in the 21st Century, at 194 (2nd edition , Wolters Kluwer 2009).

6 Brian W. Borchert, Imminent Domain Name: The Technological Land-Grab and ICANN's Lifting of Domain Name Restrictions, 45 Val.U. L. Rev. 505, 508 (2011). Available at: http://scholar.valpo.edu/vulr/vol45/iss2/3. (last visited 28 September 2011).

7 *See* Weinberg, Jonathan, Non-State Actors and Global Informal Governance - The Case of ICANN (June 7, 2010).

8 Bygrave and Bing, at 147-48 (2009).

9 *Id*. at 147 (2009). *See also* Kesan, Jay P. and Shah, Rajiv C., *Fool Us Once Shame on You - Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*. As published in Washington University Law Quarterly, Vol. 79, P. 89 at pages 167-173 (2001) (*Discussing* the history of the DNS).

10 Yahoo! Inc. Company information available at: http://info.yahoo.com/center/us/yahoo/ (last visited November 11, 2011).

(SLD).[11] A TLD refers to part of a web address making up the two or more letters after the last dot.[12] For example, in the address <www.google.com>, <.com> is the TLD. A SLD name is directly to the left of the TLD, for example <www.secondlevel.com>.[13] Traditionally, the second level has been the section of a domain name where a trademark such as Nike® is displayed (i.e.<www.nike.com>). However, a trademark may also be used at the Third Level Domain (thLD) (i.e.<www.nike.free.com>).

Currently, available open generic TLDs (gTLD), among others, include <.com>, <.net>, and <.org>. Not all gTLDs are open. For example, <.gov> is limited to the US government, and <.mil> is restricted to the US military.[14] Specialized or «sponsored» top-level domain names like <.pro> or <.jobs> represent a specific community and are also available to qualifying applicants.[15] In addition to gTLDs, country codes Top Level Domains (ccTLDs) are available. There are currently 250 ccTLDs while there are only 22 gTLDs.[16] Unlike gTLDs, the use and terms of ccTLDs are controlled, to a certain extent, by agencies in individual countries. However, the actual management of the ccTLD may be on a private basis.[17] Registration of a domain name at a ccTLD address is not necessarily open and available on a first-come-first-served-basis. Countries with catchy abbreviations, like <.co> (Columbia) and <.tv> (Tuvalu) have made their ccTLDs available for registration by private parties located outside of their countries.[18]

---

11 Efroni, Zohar, Names as Domains, Names as Marks: Issues Concerning the Interface between Internet Domain Names and Trademark Rights. Intellectual property and information wealth: issues and practices in the digital age, Peter K. Yu, ed., Praeger Publishers, 2007. Page 375. Available at SSRN: http://ssrn.com/abstract=957750.

12 Schierman, Elizabeth, *Make Room For Trademark: What you should know about the New Global Domain Names*, 53-Feb Advocate (Idaho) 25 (February 2010). AG 2.2.1.3.2 String Requirements 4. (*Providing* that «[a]pplied-for gTLD strings in ASCII must be composed of three or more visually distinct characters. Two character ASCII strings are not permitted»).

13 Weinberg, at page 4 (2010).

14 Both .gov and .mil predate ICANN.

15 Information Page for Sponsored Top-Level Domains. Available at: http://www.icann.org/en/tlds/stld-apps-19mar04/ (last visited 22 September 2011).

16 *Id*.

17 The ccTLD «.au», for example, is regulated and managed by auDA, which is a private organization that has been endorsed by the Australian Government. Swinson, John. *Domain directors PTY Ltd v .AU domain administration LTD*., comptlr 2010, 16(6), at 147-148.

18 Pfanner, Eric, *For Countries That Own Shorter Web Site Suffixes, Extra Cash From Abroad*, N.Y. Times, February 6, 2011. Available at: http://www.nytimes.com/2011/02/07/technology/07dotco.html?ref=internetcorpforassignednamesandnumbers (last visited March 25, 2011).

Like the IP numbers they represent, domain names must also be unique. The more memorable or well known a domain name is, the more valuable it generally becomes.[19] Domain names also have significance outside of their commercial application for language rights and multilingualism on the Internet.[20] New gTLDs, along with Internationalized Domain Names (IDNs), may provide new avenues for cultural and linguistic expression.[21]

Arguably, domain names are the closest thing to real property available on the Internet.[22] Therefore, in addition to cultural or linguistic value, domain names are commercially significant. Domain names corresponding with well-known or famous trademarks are highly sought after by both trademark owners and parties wishing to profit from the notoriety or recognition of a trademark.[23] Unlike trademarks, domain names also provide consumers with the exact Internet location of a business, including contact information. As many facets of the modern economy continue to move online, a company's domain name, which is often at the core of its online image, has become an increasingly important asset.[24] Although domain names are still available in existing gTLD registries, much of the beachfront property is occupied. Therefore, ICANN has decided it is time to create a bigger beach.

---

19 Manheim, Karl M. and Solum, Lawrence B., *The Case for gTLD Auctions: A Framework for Evaluating Domain Name Policy* (2003). Loyola-LA Public Law Research Paper No. 2003-11, page 27. Arguing that although there many domain names available under <.com>, many with the greatest commercial value have already been registered. Available at SSRN: http://ssrn.com/abstract=388780 or doi:10.2139/ssrn.388780 (last visited November 11, 2011). *See also* Lipton, Jacqueline, Internet Domain Names, Trademarks and Free Speech, Edward Elgar, Page 293 (2010) (*Noting* that <porn.com> was sold for almost 10 million USD).

20 Mac Sithigh, Daithi, *More than Words: The Introduction of Internationalized Domain Names and the Reform of Generic Top-Level Domains at ICANN*, pages 33-34 (June 1, 2010). University of East Anglia Law School Working Paper No. 2010-DMS-2. Available at SSRN: http://ssrn.com/abstract=1715955 (last visited November 7, 2011).

21 *Id*.

22 Lipton, at 305 (2010).

23 Manheim, Solum, at 317, 325 (2004).

24 *But see* Zittrain, Jonathan, The Future of the Internet - And How to Stop It, Yale University Press, Penguin UK/Allen Lane; Oxford Legal Studies Research Paper No. 36/2008, page 217. Available at SSRN: http://ssrn.com/abstract=1125949 (last visited 7 November 2011). Discussing the increased relevance of search engines as opposed to domain names. *See also* Thomas, Jude A., *Fifteen Years of Fame: The Declining Relevance of Domain Names in the Enduring Conflict between Trademark and Free Speech,* John Marshall Review of Intellectual Property Law, Vol. 11, page 43 (2011) (*Discussing* impact of new technologies which are less reliant on domain names). Available at SSRN: http://ssrn.com/abstract=1945374 (last visited 7 November 2011).

1.2 ICANN and the Domain Name System

The relationship between domain names, IP addresses, and the Root Server where they reside has been discussed at length in other works.[25] However, a brief discussion of the system is helpful in understandings ICANN's role in the development of domain names. In the following section, I provide a broad overview of the subject as it concerns the expansion of gTLDs.

ICANN is a private, not-for-profit entity incorporated pursuant to California law.[26] A central function of ICANN is the coordination and management of the Domain Name System (DNS).[27] ICANN took on its role as DNS administrator after entering into a Memorandum of Understanding (MOU) with the United States Department of Commerce (DOC).[28] In 2009, the DOC relinquished some of its control over ICANN when it entered into the Affirmation of Commitments (AOC). Although the amount of freedom granted under the AOC is not entirely clear, it does appear that ICANN has greater autonomy than under the previous MOU regime.[29] ICANN makes its decisions based on the input of a wide community consisting of private Internet users, businesses, governments, and an array of commercial and non-commercial interests. This bottom-up, muliti-stakeholder model is a core value of ICANN and is acknowledged in the AOC.[30] Like other recent policy decisions made by ICANN, it has implemented the Multi-Stakeholder model in the current expansion of the DNS. Consistent with that model, ICANN has incorporated advice and comments from its broad base of constituents.

---

25 Mueller, Milton, Ruling The Root: Internet Governance And The Taming Of Cyberspace, MIT Press, Cambridge, (2002).

26 Weinberg, Jonathan, *Governments, Privatization and 'Privatization': ICANN and the GAC* (February 21, 2011). Bits without borders - law, communications and transnational culture flow in the digital age, Forthcoming. Available at SSRN: http://ssrn.com/abstract=1766082 (last visited November 7, 2011).

27 *Id*. Although some alternative roots exist, the system controlled by ICANN is by far the most used and significant. *See* Bygrave and Bing, at 150 (2009).

28 Froomkin, A. Michael, *Almost Free: An Analysis of ICANN's 'Affirmation of Commitments'* (January 20, 2011). Journal of Telecommunications and High Technology Law, Vol. 9, 190-198 (2011) University of Miami Legal Studies Research Paper No. 2011-01. Available at SSRN: http://ssrn.com/abstract=1744086 (last visited 28 September 2011).

29 *See* Froomkin, at 223 (2011) (*Arguing* that the AOC fails as a contract and is more meaningful as a political document than a significant departure from prior practices).

30 Affirmation Of Commitments by the United States Department Of Commerce and The Internet Corporation For Assigned Names And Numbers. Available at: http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm (last visited September 9, 2011).

As a result of ICANN's control over available gTLDs, it plays an essential role in the expansion and evolution of the Internet.[31] ICANN does not dole out domain names itself. Rather, commercial registrars licensed by ICANN undertake the task of domain name distribution. Although ICANN does not take part in distribution of names, it does determine the TLDs that will ultimately be made available for distribution.[32] By determining the TLDs available, ICANN controls, to a large extent, what the Internet will ultimately look like to users. ICANN's decisions regarding domain names have an impact on those using the Internet.[33] There are currently over 200 million domain names.[34] What the next 200 million look like may be significantly implicated by the current expansion.

1.3 Expansion of gTLD Names

ICANN has expanded gTLD offerings on two prior occasions.[35] The first gTLD expansion occurred in 2000 and included the gTLDs <.biz> and <.info>, in addition to others.[36] In the 2000 round the ICANN board considered 44 applications for gTLDs, ultimately accepting 7 of them.[37] The process was described as «complex, expensive, and somewhat mysterious.»[38] In one article, the authors described the 2000 process as «no way to make law, sausage or domain name policy.»[39] Among other criticisms of the process, gTLD applicants had very little time to review staff recommendations and it was claimed that «the Board's discussion was based on trivial factors, such as whether a gTLD string was 'pronounceable.»[40] ICANN's failure to provide a more systematic approach, with rules that were clear and available to gTLD applicants, created problems in the 2000 round. Thus it was necessary to subsequently take a more measured and orderly approach.

31 *See* http://www.icann.org/en/about/ (last visited March 7, 2011).
32 Excluding «legacy» names pre-dating ICANN. *See* note 32 *Infra*.
33 *Id*.
34 *Id*. VeriSign, November 2010 Domain Name Industry Brief. Available at http://www.verisigninc.com/assets/Verisign_DNIB_Nov2010_WEB.pdf (last visited November 11, 2011).
35 gTLDs predating ICANN are: <.com .edu .gov .int .mil .net .org .arpa>. Prior to ICANN's existence, Jon Postel planned to introduce 150 gTLDs. See Kleinwachter, Wolfgang. *High Noon in Singapore? ICANN's new gTLD program at a crossroads* available at: http://news.dot-nxt.com/2011/05/18/high-noon-in-singapore. (last visited August 17, 2011).
36 Including gTLDs: <.aero .biz .coop .info .museum .name .pro>. List of gTLDs available at: http://www.icann.org/tlds/app-index.htm (Last visited February 11, 2011).
37 Manheim & Solum, at page 26 (2004).
38 *Id*. at 26.
39 *Id*.
40 *Id*.

A second gTLD expansion took place in 2004. The 2004 expansion was largely aimed at sponsored gTLDs, that is, domain names with restrictive eligibility requirements.[41] For example, the new gTLDs were targeted specific groups by using gTLDs such as <.travel> or <.pro>.[42] There was some tension, but also excitement regarding the gTLD <.biz>.[43] The new gTLD <.biz> was seen as a possible rival to <.com>. Although the 2004 round certainly added some choice, the names were targeted at very specific groups. Some new gTLD names like <.museum> never quite took off.[44] There was considerable discussion over the gTLD <.xxx>, which was aimed at adult themed websites.[45] Although <.xxx> was not accepted during the 2004 round, the name ultimately was accepted in 2011.[46]

As early as 2005, the Generic Names Supporting Organization (GNSO) began discussing an open round of gTLD expansion.[47] In October 2007, the GNSO completed its policy development work on new gTLDs.[48] The ICANN board of directors adopted the community-developed policy in June 2008.[49] On June 16, 2008, ICANN formally announced that it would allow new

41 *Id*. at 26.

42 Including gTLDs: <.asia .cat .jobs .mobil .tel .travel>. Available at: http://www.icann.org/tlds/stld-apps-19mar04/ (last visited February 11, 2011).

43 Wang, Minqin, *Regulating The Domain Name System: Is The «.Biz» Domain Name Distribution Scheme An Illegal Lottery?* 2003 U. Ill. L. Rev. 245, 263 (2003)(*Considering* the legality of the .biz distribution scheme). *See also* Palage, Michael, *ICANN's Implementation Recommendation Team for New gTLDs: Safeguards Needed*, Progress & Freedom Foundation Progress on Point Paper, Vol. 16, No. 10, page 2 (2009). March 2009. Available at SSRN: http://ssrn.com/abstract=1368895.

44 Levine, John, *What are TLDs Good For?*, Circle ID, (Jul 03, 2009). Available at: http://www.circleid.com/posts/20090703_what_are_tlds_good_for/ (last visited September 30, 2011). Editorial maintaining that «<.museum> is a noble failure, with only about 200 registrants, a lot of dead links, and negligible visibility.»

45 During consideration of the gTLD, ICANN received over 90000 email messages concerning the <.xxx> proposal. Comments are available at: http://forum.icann.org/lists/xxx-comments/ (last visited September 28, 2011).

46 *See* Helft, Miguel, *Pornography Sites Will Be Allowed to Use .XXX Addresses*, N.Y. Times, March 18, 2011, Available at http://www.nytimes.com/2011/03/19/technology/19domain.html?_r=1. (Discussing approval of <.xxx>) (last visited September 27, 2011).

47 The GNSO conducted their policy development process between December 2005 and September 2007. See e.g. ICANN factsheet at: http://www.icann.org/en/topics/new-gtlds/factsheet-new-gtld-program-20jul11-en.pdf (last visited August 16, 2011).

48 GNSO Final Report - Introduction of New Generic Top-Level Domains available at: http://gnso.icann.org/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm (last visited August 16, 2011).

49 Factsheet providing history of gTLDs. Available at: http://www.icann.org/en/topics/new-gtlds/history-en.htm (last visited May 11, 2011).

gTLDs and began preparations for the expansion. The first Draft Application Guidebook («AG1») was published for public comment in October 2008.[50] In the following three years, ICANN continued to release various drafts of the AG. The proposed final version of the AG («proposed final AG» or «AG5») was released in November 2010.[51] The final version was not quickly adopted as the ICANN board and members of the Governmental Advisory Committee (GAC) were unable to reach an agreement on key areas of the policy.[52] The most recent version of the AG was released on September 19, 2011, with minor changes.[53]

A clear divergence from earlier rounds is the scope of the current procedure. Unlike the 2000 and 2004 rounds, it is expected that hundreds of new gTLDs may be created. As noted by one author, it «has been one of the most contentious and longest running disputes at ICANN.»[54] Unlike the 2000 and 2004 rounds, with pre-determined offerings, the current «wide-open» expansion has brought with it a measure of concern, particularly for trademark holders.[55] The open approach to new gTLDs may provide with it many benefits consistent with ICANN's goals of increased innovation. For businesses and individuals that missed out on the initial gTLD rounds, the expansion may also provide something of a second chance for a stronger online presence.[56] Applicants may also be interested in entering the registry or registrar market.[57] Parties able to secure a popular gTLD will likely have an opportunity for increased SLD name sales.[58] Companies that secure their own TLD domain will no longer have to fight to obtain the domain name of choice for advertising campaigns.

---

50 Rosette, Kristina, *ICANN And Trademark Protection in New GTLDs*, Trademark World #223, December 2009\January 2010. AG1 available at: http://www.icann.org/en/topics/new-gtlds/draft-rfp-24oct08-en.pdf (last visited May 11, 2011).

51 AG5 available at: http://www.icann.org/en/topics/new-gtlds/draft-rfp-clean-12nov10-en.pdf (last visited May 11, 2011).

52 ICANN\GAC scorecards. Available at: http://meetings.icann.org/board-gac-spring11 (last visited September 28, 2011).

53 Applicant Guidebook Sept 19, 2011. Available at http://www.icann.org/en/topics/new-gtlds/rfp-clean-19sep11-en.pdf (last visited September 30, 2011).

54 Froomkin, at 225 (2011).

55 Farley, Christine Haight, *Convergence and Incongruence: Trademark Law and ICANN's Introduction of New Generic Top-Level Domains*, John Marshall Journal of Computer & Information Law, Vol. 25, No. 4, 2009, American University, WCL Research Paper No. 2009-22. Available at SSRN: http://ssrn.com/abstract=1400304. (*Stating* that gTLD choices are so wide they could literally be «dot anything.»).

56 Borchert, at 506 (2011) (*Maintaining* that consumers and businesses are being provided with a second chance for a land-grab»).

57 Froomkin, at 225 (2011).

58 *Id*.

Like previous rounds, not all groups with an interest in the Internet have welcomed the proposition of expanded gTLDs.[59] Advocates from the business community, trademark holders, and governments via the GAC have voiced concerns regarding the potential negative impact of new gTLDs.[60] Businesses and trademark holders argue that after expending a great deal of energy and resources to secure their domain names and online identities, new gTLDs will bring with them new expenses.[61] Anticipated expenses include, but are not limited to expenses related to increased cybersquatting.[62] Associations of trademark holders maintain that their members will be required to undertake an unprecedented number of «defensive registrations» to protect their trademarks.[63] Rights holders also maintain that revisiting legal battles with cyber-squatters and possible other infringers of their rights will bring significant operating costs, which will ultimately be carried by consumers.[64] In recent testimony before a US congressional committee, Mei-lan Stark, senior vice president for intellectual property at Fox News Corporation, testified that as a result of the new gTLDs, protection of their brand might cost as much as «$12 million in the initial stages alone.»[65]

Potential expenses to rights holders are often difficult to ascertain. Although business representatives assert that the cost will be substantial, estimates vary widely. For example, one study projects the cost to trademark owners as be-

59 Palage, at 1 (2009). *See also* Palage, Michael, *Top Three Reasons to Just Say No to ICANN's Current EOI gTLD Proposal*, The Progress & Freedom Foundation Progress Snapshot, Vol. 6, No. 3, (2010). Available at SSRN: http://ssrn.com/abstract=1619468 (last visited September 28, 2011).

60 *See* GAC scorecard on new gTLD outstanding issues listed in the GAC Cartagena Communiqué. Available at: http://icann.org/en/topics/new-gtlds/gac-scorecard-23feb11-en.pdf (last visited March 10, 2011).

61 Pelage, at 1 (2009).

62 See Zhao, Yun., Dispute Resolution in Electronic Commerce, Martinus Nijhoff Publishers, at 178 (2005). See also Hörnle, Julia., *The Uniform Domain Name Dispute Resolution Procedure: Is Too Much Of A Good Thing A Bad Thing?* 11 SMU Sci. & Tech. L. Rev. 253, 254 (2008).

63 Palage, Michael, *ICANN's 'Go/No-Go' Decision Concerning New gTLDs,*. Progress & Freedom Foundation Progress on Point Paper, Vol. 16, No. 3, February 2009. Available at SSRN: http://ssrn.com/abstract=1368883. WIPO estimates that nearly 90% of Corporate registrations are defensive. Available at: http://www.wipo.int/amc/en/docs/felman23.pdf) (last visited May 10, 2005).

64 *Id*.

65 Testimony of Mei-lan Stark, senior vice president for intellectual property at News Corp.'s Fox Entertainment Group.http://www.nytimes.com/2011/06/20/technology/20ihtcache20.html?pagewanted=1&_r=1&sq=ICANN&st=cse&scp=2. (last visited June 20, 2011).

ing as little as .10 USD per trademark registered worldwide.[66] In much of the discussion surrounding gTLD expansion, great expenses to rights holders are assumed. Trade associations, among other groups, have consistently charged that gTLDs will be enormously costly.[67] However, the overall economic impact and costs of new gTLDs is far from certain. ICANN's studies on the economic impact of new gTLDs have thus far been inconclusive. In one such report, ICANN simply stated that «[n]one of the studies were able to specifically quantify projected net benefits, stating, among other things, that innovation was difficult or impossible to predict, as was the effectiveness of the many cost mitigation tools being implemented along with the program.»[68] This is, at least in part, due to the difficulty in determining how consumers will react to the expansion. The threat of new gTLDs to existing domain names largely depends on success of the new gTLDs. The prime gTLD space may well remain at <.com>.[69] If the new gTLDs are not used, any threat they pose to brand strength trademark holders will likely be reduced.

1.4 Domain Names and Disputes

The interests of intellectual property rights holders and the allocation of domain names have been a source of conflict that has played out in mediation, arbitration, and courtrooms since the early1990s.[70] In the present expansion, issues of import to trademark holders have been central to discussions surrounding new gTLDs. There are several reasons that issues relating to trademarks have been given such prominence. In addition to having deep pockets, trademarks have a fairly extensive legal history. Despite the wide use of

66 Krueger, Fred and Van Couvering, Antony, *Quantitative Analysis of Trademark Infringement and Cost to Trademark Holders in New gTLDs*. Minds + Machines Working Paper 2010-1, (February 10, 2010).
Available at: http://www.mindsandmachines.com/wp-content/uploads/M+M-Quantitative-Analysis-of-Cost-of-New-TLDs-to-Trademarks.pdf (last visited August 15, 2011).

67 *See* Association of National Advertisers (ANA), *87 Major Assns. and Businesses Join with ANA to Form Coalition to Oppose ICANN's TLD Expansion Program* (2011) , Available at: http://www.ana.net/content/show/id/22351 (last visited November 11, 2011).

68 Available at: http://icann.org/en/topics/new-gtlds/market-economic-impacts-15apr11-en.pdf (last visited May 15, 2011).

69 Lipton, at 79 (2010) (*Arguing* that based on past releases of new gTLDs, <.com> will likely remain the most sought after gTLD).

70 Lipton, Jacqueline D., *Beyond Cyber squatting: Taking Domain Name Disputes Past Trademark Policy*. Wake Forest Law Review, Vol. 40, No. 4, at 12-13(2005). Providing background on the rise of domain name disputes in the 1990s. Available at SSRN: http://ssrn.com/abstract=770246 (last visited September 28 2011).

domain names, there is no uniform approach to their legal nature.[71] In some jurisdictions, domain names are treated as a form of intangible property.[72] Other jurisdictions have deemed domain names as merely a contract right.[73] Particularly in the US, the treatment has been different depending on the property claim asserted.[74] Trademarks, on the other hand, benefit from a more consistent legal treatment.

Having a broad base of prior litigation and statutory history, the path traveled by trademarks is in many ways easier to follow. As a result, courts and policy makers often attempt to push domain names into the more established trademark mold. Although convenient, the efficacy of treating domain names as automatic extensions of trademarks raises questions.[75] While they certainly share some characteristics of trademarks, domain names are not always a good fit within general trademark principles.[76] Principally, the review process before a trademark is granted is fairly extensive in the majority of jurisdictions.[77] Domain names can often be registered online within a matter of minutes. The more descriptive a domain name, the more valuable it generally becomes. On the other hand, inclusion of a trademark term in common vernacular, making it generic in its use, threatens its grant of exclusivity.[78]

A core aspect of the tension between trademarks and domain names is the global accessibility and presence of domain names.[79] Domain names remain the same regardless of their physical location. Trademarks are territorial and are granted protection within a geographically defined area, which is often

71 Marinković, Ana Rađki. *Domain Names: Towards A New Form Of IP Right*, Oxford Journal of Intellectual Property Law & Practice, at 60-63 (2011).

72 *Kremen v Cohen*., 67 USPQ 2d 1502 (9Th Cir. 2003).

73 *See* Burshtein, Sheldon, *Is A Domain Name Property?*, Oxford Journal of Law & Inl of Intellectual Property, Vol. 1, Issue1 pp. 59-63, 59 (2011).

74 Daniel Hancock, Note, *You Can Have It, But Can You Hold It?: Treating Domain Names as Tangible Property*, 99 Ky. L.J. 185, 188-194 (2011). Available at: http://kljo.org/48. (last visited September 28, 2011).

75 *See* Komaitis, Konstantinos, *Trademark Law's Increment Through the Uniform Domain Name Dispute Resolution Policy*, Oxford Intellectual Property Law and Practice, Vol. 6, No.8 (2011).

76 Greenberg, Daniel and Speres, Jeremy, *.Com v Trade Marks: Who Will Win?*, Oxford Journal of Intellectual Property Law & Practice, Vol.5, No.4., 268-281, 274 (2010).

77 *Id*.

78 If a mark becomes generic, exclusivity is lost. For example «'Aspirin', 'cellophane', and 'linoleum' began as trademarks and are now generic.» Gordon, Wendy J., *Intellectual Property*. As published in The Oxford Handbook Of Legal Studies, Peter Cane and Mark Tushnet, eds., Oxford University Press, at 617-646, (2003). Available at SSRN: http://ssrn.com/abstract=413001 or doi:10.2139/ssrn.413001(last visited September 28, 2011).

79 *See* Efroni, at 377 (2007)(*Stating* that the «friction between trademark law and domain names is an inevitable outgrowth of the Internet.»).

further narrowed to a product or service class. Goods or services promoted under a trademark may be substantially different from one geographic location, or product class, to the next. As a result, the same trademarked term may be given protection to entities located in different parts of the world. Stated differently, the exact word or phrase may be legitimately trademarked by multiple individuals or entities at different locations. The point of departure is that the law does not «protect the mark *per se* but the combination of the mark's symbolic character and its goodwill.»[80] Requiring this combination of factors allows for the same words to be used in different classes or product areas.

Because domain names must be unique, only one domain name identical to a trademark may be granted. Domain names, taken alone, are often considered to be «non-distinctive» in character.[81] As a result, they often fall outside the protections provide by trademark law. However, even if the word or phrase making up the domain name is not distinctive, or it fails to fully convey the value of the mark, domain names are still significant to trademark owners as an expression of their trademark or online image.[82] It has also been argued that the focus of trademark protection on the Internet may be shifting from its traditional basis of protecting an expression of goodwill, to focusing solely on a word or phrase.[83]

Part of the tension that has traditionally existed between trademarks and domain names may lie in the inconsistent definition or treatment of the right incorporated into a domain name.[84] If a domain name is purely a right under contract, the remedies available to the domain name holder may be defined narrowly in the contractual document. If that is the case, the rights of a domain name holder are potentially more limited. If the right is broader, and it embodies either a self-standing property right, or an expression of a property right, the rights of a domain name holder, including due process rights, are arguably greater than under than under a contractual arrangement. The question of what process is due the domain name holder, to protect their underlying right, is not always clear. In the present expansion scheme, the rights of a gTLD applicant, as opposed to those of a domain name holder, may also be distinguishable. In the next section, discussion will move to some of the systems used to adjudicate rights of domain name holders.

80 Komaitis, at 555 (2011).
81 MacQueen, Hector, Waelde, Contemporary Intellectual Property Law and Policy., Page 674 (Oxford Press 2007). *See also Nastionsbanc Montgomery Securities LLC's Application*, [2000] ETMR 245.
82 *Id*.
83 Komaitis, at 559 (2011).
84 Marinković *supra* note 71.

1.5 Resolving domain name disputes in the DNS

Uncertainty regarding applicable law, coupled with jurisdictional and language barriers, has led ICANN to create systems for resolving domain name disputes. In 1999, ICANN drafted the UDRP as a means of combating cyber squatting and quickly resolving disputes over domain names.[85] In past expansions of gTLDs systems to resolve disputes have also been used. In the present expansion, procedures for resolving disputes are included at several points in the AG, in addition to module 3.[86]

Like other systems of dispute resolution, systems for domain name arbitration or dispute resolution developed by ICANN share the goal of «seeking to apply justice.»[87] The UDRP has been widely used in domain name disputes so it provides a useful point of comparison. The focus of this section is on the role of the dispute resolution procedure provided for in module 3 of the AG. The UDRP includes both the procedural and substantive law applicable in disputes. As a system of dispute resolution, the UDRP is often characterized as a form of non-binding online arbitration.[88] However, there is not consensus on this point. It has also been argued that referring to the UDRP as an arbitration proceeding is a «common mistake» as «the UDRP is confusingly similar to arbitration as it resembles its nature, but neither serves justice nor facilitates the parties' needs.»[89]

The UDRP procedure is drafted in a concise manner and provides a specific and limited remedy. If a party registers a domain name that is identical or confusingly similar to a trademark; without a legitimate interest in the domain name, then a trademark owner may seek to have the name transferred.[90] The UDRP's jurisdiction is derived from ICANN's near monopoly over the DNS.[91]

---

85 Hörnle, Julia, Cross-border Internet Dispute Resolution, Cambridge University Press, at 187 (2009).

86 AG 5.4.1. Providing registry operator requirements for implementation of Uniform Rapid Suspension (URS) procedure and Trademark Post-Delegation Dispute Resolution Policy (PDDRP).

87 Komaitis, Konstantinos, The Current State of Domain Name Regulation: Domain Names As Second Class Citizens In A Mark-Dominated World, Routledge, at 85 (2010).

88 Kaufmann-Kohler, Gabrielle and Schultz, at 6 (2010) (*discussing* the extensive use of the process and the low number of UDRP appeals). Available at SSRN: http://ssrn.com/abstract=896881(last visited September, 28 2011).

89 Komaitis, at 89-91 (Routledge 2010). *See* Kaufmann-Kohler & Schultz, at 38 (2004) (*Stating* that the UDRP is not true arbitration pursuant to US law). *See also* Dluhos v. Strasberg, 321 F.3d. 365, 372 (3rd Cir. 2003).

90 Procedure available at: http://www.icann.org/en/dndr/udrp/policy.htm (last visited March 23, 2011).

91 Bettinger, Torsten. Domain Name Law and Practice, page 947 (Oxford 2005).

A prevailing party's remedy is limited to the transfer of the domain name.[92] Private dispute resolution providers administer all UDRP disputes.[93] If a party does not agree with the decision rendered by a dispute resolution provider, they have the option of pursuing the matter in court on a *de novo* basis.[94]

Acceptance of the UDRP procedure is a condition precedent to obtaining a gTLD. The legal basis for the UDRP is grounded in the contract entered into by the domain name holder, rather than as law created by a specific state or jurisdiction.[95] Because the UDRP clause is required, an individual seeking a domain name does not have the ability to negotiate or disagree with the term. Stated differently, the UDRP requirement is presented to potential domain name owners on a take it or leave it basis. In the case of ccTLDs, the UDRP is not required, but has been adopted in some instances.[96]

The UDRP procedure has received much attention from legal scholars because it is a functioning and widely used system for settling disputes. The UDRP generally receives high grades for being fast, flexible, and inexpensive.

---

92 Thornburg, Elizabeth G., Fast, *Cheap & Out of Control: Lessons from the ICANN Dispute Resolution Process*. Journal of Small & Emerging Business Law, Vol. 7, (2001)(«Because ICANN has a contract with the company that controls the root server that assigns domain names, it has the power to enforce the arbitrators' decisions without the need to ask a court to enforce the judgment.»). Available at SSRN: http://ssrn.com/abstract=321500 or doi:10.2139/ssrn.321500 (last visited September 28, 2011).

93 There are currently three disputer resolution providers including: (1) WIPO, (2) Asian Domain Name Dispute Resolution Centre, (3) The Czech Arbitration Court Arbitration Center for Internet Disputes. List of ICANN approved providers available at: http://www.icann.org/en/dndr/udrp/approved-providers.htm (last visited March 23, 2011).

94 Sorkin, David E., Judicial *Review of ICANN Domain Name Dispute Decisions*. Santa Clara Computer and High Technology Law Journal, Vol. 18, No. 1, pp. 35-55, 46 (2001) (*Citing Strick Corp. v. Strickland*, 162 F. Supp. 2d 372 (E.D. Pa. 2001)). Available at SSRN: http://ssrn.com/abstract=1057761 (last visited September 29, 2011). *See* Barcelona.com, Incorporated v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 626 (C.A.4 (Va.),2003)(*Discussing* applicability of de novo standard).

95 Helfer, Laurence R. and Dinwoodie, Graeme B., *Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy*. William & Mary Law Review, Vol. 43, p. 141, 149 2001; Stanford/Yale Jr. Faculty Forum Paper No. 01-05. Available at SSRN: http://ssrn.com/abstract=275468 (last visited September 29, 2011)(*Providing* that «[n]either the UDRP's substantive content nor its prescriptive force necessarily depend upon the laws, institutions, or enforcement mechanisms of any single nation-state or treaty regime.»). *See also* Schultz, Thomas, *The Roles of Dispute Settlement and ODR ADR In Business: Practice And Issues Across Countries And Cultures*, K Arnold Ingen-Housz, ed., Kluwer Vol. 2, pp. 135-155, 153 (2011)(*Stating* that the UDRP procedure is «purely contractual in nature and not arbitral»). Available at SSRN: http://ssrn.com/abstract=1811890 (last visited September 28, 2011).

96 ccTLDs may apply the terms of UDRP in their registration policy, but they are not required to do so.

However, the speed and flexibility process have also been characterized as «fast, cheap & out of control.»[97] The UDRP has a simple substantive structure. It does not require lawyers and it moves quickly from the initial filing until final resolution.[98] Perhaps most importantly, the UDRP provides parties with an alternative to the court system. As noted by one author, «[US] federal civil trials can drag on for months or even years, UDRP proceedings last about two months on average.»[99] Despite many praises, the UDRP has also been faulted for failing to provide adequate due process and focusing too heavily on the issues germane to commercial speech and trademarks. [100]

The UDRP has been widely utilized by trademark holders as a means of combating various unauthorized use of trademarks as domain names.[101] The UDRP has also been considered very successful process for trademark owners, possibly at the expense of lawful registrants.[102] The UDRP has allowed trademark owners to challenge abuses, particularly cyber squatting, and protect their legal rights on an international scale. Because laws governing trademark rights are largely based on territorial principles, they are not well suited for the Internet.[103] Where infringements occur, and what law is applicable, is often central to exercising jurisdiction.[104] On the Internet, it is often difficult to determine exactly where things happen. From a practical perspective, it may be difficult for a court to provide a cross boarder remedy as a result of the extraterritorial effect any remedy may contain.[105]

By creating a system for resolving disputes online, regardless of the party's location, the UDRP provides trademark owners with a valuable tool. Furthermore, the simple pleading procedures and rapid time tables make the UDRP an efficient means for resolving domain name disputes, at least from

97 Thornburg, at 191 (2001).

98 Ryan Owens, Note, *Domain-Name Resolution After Sallen v. Corinthians Licenciamentos & Barcelona.com, Inc. v. Excelentisimo Ayuntameiento de Barcelona*, 18 Berkeley Tech. L.J. 257, 265 (2003).

99 *Id*.

100 See note 95 *Supra*. *See also* Lipton, at 12-13 (2005).

101 Efroni, at 387-388 (2007) (*Stating* that «panels have decided on thousands of domain name disputes»).

102 Kaufmann-Kohler, Gabrielle and Schultz, Thomas, *Online Dispute Resolution: Challenges for Contemporary Justice*, page 39 (2004)(*discussing* the extensive use of the process and the low number of UDRP appeals).

103 Helfer and Dinwoodie, at 150 (2001).

104 *Id*. *See also* Bettinger, at 1167 (2005). «The conflict-free coexistence of confusingly similar signs based on the existence of separate geographical territories becomes impossible where signs are used on a website on the Internet, because such a site is, for technical reasons, necessarily accessible around the world.»

105 Bettinger, at 1167 (2005) (*Citing* Berlin District Court, 1997 CR 685 ff).

a trademark holder's perspective. Whether the UDRP design promotes or comports with notions of due process and fairness continues to be debated.[106] Central criticisms of the UDRP have been that it lacks an appellate process, the right to respond is limited, and that it can be difficult to access, particularly when the respondent lacks legal sophistication or English language skills. By allowing the party filing the complaint to choose the forum, some commentators have questioned whether the process allows for forum shopping.[107]

In the next section, I consider the DRP in the AG and make some comparisons to the UDRP. At the onset, it is worth noting that the UDRP policy has some significant differences from the module 3 policy provided for in the AG. Unlike the UDRP, module 3 takes place prior to the domain name being issued. At the point module 3 may be utilized, the applicant has not been granted use of or any rights to a new gTLD. The UDRP policy considers complaints under a much different distribution system. Unlike the new gTLD process, the UDRP does not consider domain names that are subject to a pre-approval, high application fees, or a lengthy application process. The names being challenged pursuant to the UDRP have been issued on a first-come first-served-basis.[108]

2 Application of the gTLD Dispute Resolution Procedure (DRP)

2.1 Introduction

Minimization of conflict by design has been a central theme in creation of the new gTLD application process. Based on its experiences during the gTLD expansions of 2000[109] and 2004,[110] ICANN gained insight into the legal, technical, and political conflicts inherent in domain name expansion.[111] As a result, ICANN is arguably in a much better position to implement a dispute reso-

106 Hörnle, Julia.,11 SMU Sci. & Tech. L. Rev. 253, 257-261 (2008).

107 P. Kesan & Andres A. Gallo, *The Market For Private Dispute Resolution Services-An Empirical Re-Assessment Of ICANN-UDRP Performance*, 11 Mich. Telecomm. & Tech. L. Rev. 285, 368-69 (2005) (Discussing studies of the UDRP).

108 *See* Reed, Shiveh Roxana, *Sensible Agnosticism: An Updated Approach To Domain-Name Trademark Infringement*, 61 Duke L.J. 211, 222-25 (2011) (*Discussing* the ease of the registration process on a first-come, first-served basis).

109 Information including applications and guidebooks from the 2000 round available at: http://www.icann.org/en/tlds/app-index.htm (last visited 11 May 2011).

110 Information including applications and guidebooks from the 2004 round available at: http://www.icann.org/en/tlds/stld-apps-19mar04/ (last visited 11 May 2011).

111 In particular, the contentious debate around the <.xxx> domain name tested ICANNs resolve against individual nation states and its own processes for review.

lution system that is procedurally effective. Debate over whether the *ex ante* approach taken with the module 3 procedure of the AG provides trademark holders with sufficient protection are ongoing. In evaluating the model 3 system, some comparison to the *ex post* approach taken by the UDRP is useful. In addition to the systems, I will also consider some practical questions including whether the procedure ought to be amended to provide more guidance to dispute resolution providers and clearer standards for parties to follow.

All new gTLD applications are subject to the objection-based dispute resolution procedure in module 3 of the AG.[112] Like the UDRP, ICANN's authority to require the module 3 DRP is derived from its monopoly over the DNS system.[113] ICANN's jurisdiction, and its ability to enforce decisions, is contractual.[114] By allowing objections early in the process, ICANN has provided interested parties with multiple opportunities to protect intellectual property like trademarks. The dispute resolution system also allows states, via the GAC, protection from new gTLDs «that are identified by governments to be problematic.»[115] The GAC objection may be used to block new gTLDs using names or phrases that may violate national law or otherwise raise national sensitivities.[116]

2.2 Overview of the Procedure

Applications for new gTLDs must pass a rigorous administrative check. Applicants must also pay an 185,000 USD application fee.[117] Applications that pass the administrative check will then be posted on the ICANN website for public comment. The comment period allows members of the Internet community, without any specific interest, to raise concerns regarding new gTLDs. Following the comment period and background screening, ICANN will conduct its Initial Evaluation (IE) of gTLD name applications. In conducting the IE of new gTLDs, the reviewing body will consider a variety of issues sur-

112 «Objection Procedures,» Module 3., Applicant Guidebook, Discussion Draft (April 2011) § 3-1.

113 *See* Bettinger, at page 947 (2005).

114 Shahan, Travis, *The World Summit on the Information Society & the Future of Internet Governance*, Computer Law Review & Technology Journal, Summer, 10 Computer L. Rev. & Tech. J. 325, 334-335 (2006) (*Discussing* contracts and agreements surrounding the DNS).

115 AG at. 3.1.

116 *Id*.

117 *See* AG at 1.5.1. GTLD evaluation fee is required from all applicants, but if an application is rejected at an early stage, or withdrawn, a partial refund may be available.

rounding the application including similarity to existing applications, DNS stability, and use of geographic names.

After the results of the IE are announced, parties have two weeks to make objections. There are two basic procedural requirements for an objection, in addition to paying required fees.[118] First, the objection must be timely. Second, the objecting party must have standing.[119] Standing requirements essentially encompass three functions including general eligibility to make an objection, the objections available to a party, and to determine the dispute resolution service provider that will consider the objection.[120]

The objecting party bears the burden of proof during the entire process.[121] Claims available to a third-party are dependant on the legal rights of the objecting party. If a third-party has a sufficient basis for an objection on more than one ground, they may include a combination of objections, or even make multiple objections arising from the same circumstances. However, the objections must be made to the appropriate provider. In addition to objections based on specific rights, ICANN has added *a GAC Advice on New gTLDs* procedure to module 3. The GAC objection provides GAC members the opportunity to make a formal (or equivalent) objection, even though they would not meet general standing requirements set out in module 3.

If an objection is successful, the new gTLD will be ineligible for further review and will not be issued. For the party applying for a new gTLD, this determination is dispositive. There is no appeal provided for in this step of the process. However, the party seeking a new gTLD may apply in subsequent rounds. For the party making the objection, the dispute resolution is only one of several available measures to protect their rights. If the objector does not succeed with their opposition to a new gTLD at the application stage, affected parties will still have UDRP and other Rights Protection Measures (RPMs) available.[122] However, after the gTLD is issued, there is no clear avenue for the objecting party to stop or «block» the new gTLD from proceeding.

118 AG at 1.5.2. Dispute Resolution Filing Fee will be required to file a formal objection, and any response to the objection. ICANN estimates that filing fees from USD 1,000 to USD 5,000, per party, per proceeding. Dispute resolution service providers will determine their own fee structure.

119 DRP Art. 1 (d). Providing for derogation of the procedure only with the express consent of ICANN.

120 AG at 3.0-3.1. Dispute Resolution Procedures. AG at. 3.1.1 Grounds for Objection. AG at. 3.1.2 Standing to Object.

121 AG at 3.5.

122 AG at 5.4.1.

2.3 Objection based on confusion between potential gTLD «string» and an existing or applied for gTLD

During the background screening, ICANN will check gTLD applications for string similarity.[123] The string similarity review will use an algorithm that is designed to help ICANN flag applications for removal that fail to meet minimum gTLD requirements.[124] Domain names that compromise DNS stability or use geographic names without proper authorization will not be issued. Background screening for string similarity will not weed out all potentially problematic or confusing applications. Clever spellings or code words may escape the string similarity review.

In anticipation of this shortcoming, ICANN has developed a system for interested parties to object to confusing applications based on their similarity to existing or applied for gTLDs.[125] Standing to object to gTLDs that are confusingly similar is limited to current gTLD operators and applicants applying for a gTLD in the same round of applications.[126] A string confusion objection may be based on confusion between an applied-for gTLD and a currently operating gTLD.[127] If an existing gTLD operator is successful with their objection, the application will be rejected.[128] If, on the other hand, the complainant is another gTLD applicant, their applications will be placed in a «contention set» and will be subject to procedures covered in module 4 of the AG.[129]

Both the procedural and substantive rules governing string confusion objections can be found in module 3 of the AG. In an attachment to the module, the AG provides the dispute resolution procedure to be applied by dispute resolution service providers (DRSPs). However, the standards provided are not entirely consistent. Pursuant to module 3 of the AG, the grounds for a string confusion objection are where «[t]he applied-for gTLD string is confusingly similar to an existing gTLD or to another applied for gTLD string in the same round of applications.»[130] The standard for prevailing on a string confusion objection is where «…a string so nearly resembles another that it is *likely* to

123 AG at 3.4. *See* gTLD DRP Art.2(e)(i). «String Confusion Objection refers to the objection that the string comprising the potential gTLD is confusingly similar to an existing top-level domain or another string applied for in the same round of applications.»

124 *See* http://icann.sword-group.com/algorithm/ (last visited September 22, 2011)(*providing* example of algorithm used to determine similarity.»).

125 All objections based on string confusion must be filed within the two-week period after the results of the IE are posted.

126 AG at 3.5.1

127 AG at 3.2.1.

128 AG at 3.2.2.1.

129 *Id*. (*referring* to «Contention set proceedings» in Module 4 of the AG).

130 *Id*. Emphasis added.

deceive or *cause confusion.*»[131] The AG further requires that that it is «*probable*, not merely *possible* that confusion will arise in the mind of the average, reasonable Internet user.»[132]

Based on the standard provided for in the AG, mere association with another string will not be sufficient to support a finding of string confusion by a dispute resolution service provider.[133] This is for two main reasons. First, the AG requires that in addition to being «confusingly similar,» the confusion must be «likely.»[134] Second, the AG provides an objective measure, «the reasonable Internet user,» to determine whether the likelihood of confusion is great enough that it is «probable» rather than simply «possible.»[135] Unlike the UDRP, there is no requirement of «bad faith» on behalf of the party applying for the new gTLD.[136] Likely confusion, in the eyes of «the reasonable Internet user» to an existing or applied for gTLD is sufficient for the objecting party to prevail.

The attachment to module 3 includes a summary version of the dispute resolution procedure to be applied by a DRSP. Unlike the AG explanation, the attachment provides a condensed format. Much of the detailed description provided for the in AG is left out. In addition to being shorter, the attachment is not entirely consistent with module 3. Pursuant to the attachment, if the new gTLD is «confusingly similar» to another existing or applied for gTLD, the application will be denied.[137] Unlike the AG, the attachment does not contain the expanded qualification that the new gTLD must be «*likely* to deceive or cause confusion.» Further, the objective «reasonable Internet user» standard is not included. The attachment does not reference any a specific document to be applied in disputes.[138] The attachment merely provides that the hearing panel «shall apply the standards that have been defined by ICANN for each category of Objection» and refers back to the confusingly similar standard in the same document.[139]

In the event of a discrepancy between AG module 3, and the attachment, the attachment will prevail.[140] Although the attachment does state that the

131 AG at 3.5.1. Emphasis added.
132 *Id*. Emphasis added.
133 AG at 3.5.1.*See also* AG at. 2.2.1.1.2. *See* Schierman, at 25 (2010).
134 AG at 3.5.
135 *Id*.
136 UDRP Rules available at: http://www.icann.org/en/dndr/udrp/policy.htm (last visited September 20, 2011).
137 AG attachment at Art.2(e)(i)(«confusingly similar to an existing top-level domain or another string applied for in the same round of applications»).
138 AG Attachment.
139 AG Attachment at Art.20 Standards.
140 AG at 3.3. Referenced as the «Procedure» in the AG.

«…panel shall apply the standards that have been defined by ICANN,» exceptions are provided.[141] For example, in addition to the standards specifically provided for, a DRSP «may refer to and base its findings upon the statements and documents submitted and *any rules or principles* that it determines to be applicable.»[142] By including «any rules or principles that it determines to be applicable» the rules applied by the DRSP have the potential to deviate from those provided for in the AG and those enumerated in the attachment.[143]

Although the attachment seems to provide more flexibility than the AG, it is not inconsistent with the flexibility built into other parts of the AG. The AG also provides the DRSP with a great deal of flexibility when determining the standard they will follow. Regarding the standards to be applied, the AG provides that «[t]he panel may also refer to other relevant rules of international law in connection with the standards.»[144] Like the attachment standard, the AG also provides DRSPs with a large amount of leeway to determine which «international law» they will ultimately choose to apply. Although the AG is voluminous, and in many ways resembles an omnibus approach to new gTLDs, it is not exhaustive at least regarding dispute resolution.

The UDRP faced similar criticism regarding the clarity of the standards to be applied. In pursuing its goal of providing a summary process, the UDRP arguably failed to provide adequate guidance to dispute resolution service providers. Critics maintain that by failing to set out clear standards, both procedurally and substantively, the UDRP lacks necessary due process protections. A consequence of unclear standards for the UDRP has been the application of diverging approaches by dispute resolution providers.[145] Under the attachment approach, it is arguable that a different result could be reached, depending on whether the DRSP applies the standard set forth in the attachment, the standard provided in the AG, or applies a standard derived from an international source. In the next section, I will discuss the diverging standards and the potential outcome they may have.

141 *Id*. at Art.20(a)(*referencing* standards in Art. 2(e)(i)).
142 *Id*. at Art.20(b). Emphasis added.
143 *Id*. Art.20 *Standards*.
144 AG at 3.5.
145 Chik, Warren Bartholomew Kam Wai, *Lord of Your Domain, But Master of None: The Need to Harmonize and Recalibrate the Domain Name Regime of Ownership and Control,* International Journal of Law and Information Technology, Vol. 16, Issue 1, pp. 8-72, at 19 (2008).

2.4 Applicable Standard: Does the discrepancy matter?

The «confusingly similar» standard is widely applied in trademark law and domain name disputes.[146] The US Anticybersquatting Consumer Protection Act creates a cause of action for «bad faith» registrations that are «confusingly similar» to a trademark.[147] The UDRP uses a similar standard and allows transfer of a domain name that is «identical or *confusingly similar* to a trademark or service mark …»[148] However, for a complainant to prevail under the UDRP; the objector must also show the registrant has no legitimate interest in the domain name and that the name is registered in bad faith.[149] The adoption of a simplified «confusion test» for evaluating domain names, particularly in the UDRP, has not been without criticism. As stated by one author:

> *This rule [the confusion test] is 'borrowed' and is in conformity with the language used in traditional trade mark law statutes; however, the way it is interpreted and applied departs significantly from the way it is used by courts and tribunals. A combination of lack of direction on behalf of ICANN—as the administrator of the Policy—and of the World Intellectual Property Organization (WIPO)—as the mastermind behind its inception and an accredited dispute resolution provider— have twisted the 'confusion test' to its core.*[150]

Whether adoption of a similar test for evaluating new gTLD applications, and application of the test by the DRSP will result in similar inconsistencies or

146 See *Infra* note 153.
147 15 U.S.C. § 1125 (d)(1)(c)(2006). *See* The Utah E-Commerce Integrity Act. Utah Code Ann. § 13-40-101 (2010)(prohibiting cybersquatting at a state level).
148 UDRP Art. 4(a)(i).
149 *Id*. at 4(a)(ii-iii).
150 Komaitis, at 560 (2011).

problems, is an important point of consideration.[151] This is particularly so if the standard is taken out of context or applied in an oversimplified manner.[152]

In the US, infringement of a trademark is based on «whether trademark is such 'as to be likely, when used on or in connection with the goods of such other person, to cause confusion, or to cause mistake, or to deceive.'»[153] Thus, the «likelihood of confusion» standard also considers how a mark is used, not just its similarity to other marks, before finding a basis for infringement.[154] Some UDRP providers, following the US approach, have applied a similar test when determining whether a domain name is *confusingly similar* pursuant to UDRP Art. 4(a).[155] In the current AG, unlike the dispute resolution procedure provided for in the module 3 attachment, the legal standards are combined. The AG standard blends the «likelihood of confusion» standard with the «confusingly similar» standard.[156] It is unclear whether the blending of the legal standards will have any effect on the procedural or substantive rights of the parties seeking dispute resolution.

The «confusingly similar» standard in the attachment and «likely to deceive or cause confusion» set forth in the AG are not the same legal standard.[157] Lack of clarity regarding the standard to be applied could be a potential barrier to releasing new gTLDs.[158] Under a broad reading of the «confusingly similar» standard, it may be difficult for new gTLDs to overcome objections,

151 *Id*. Discussing the lengthy evaluation taken under US law for a finding of infringement based on confusion—an evaluation that includes the following factors: «(i) the similarity or dissimilarity of the marks in their entireties as to appearance, sound, connotation and commercial impression; (ii) the similarity or dissimilarity and nature of the goods described in an application or registration or in connection with which a prior mark is in use; (iii) the similarity or dissimilarity of established, likely-to-continue trade-channels; (iv) the conditions under which and buyers under whom sales are made; (v) the fame of the prior mark; (vi) the number and nature of similar marks in use on similar products; (vii) the nature and extent of any actual confusion; (viii) the length of time during and the conditions under which there has been concurrent use without evidence of actual confusion; (ix) the variety of goods on which a mark is or is not used; (x) the market interface between the applicant and the owner of the prior mark; (xi) the extent to which the applicant has a right to exclude others from use of its mark on its goods; (xii) the extent of potential confusion; and (xiii) any other established fact probative of the effect of use.»

152 *Id*.

153 Farley, at 627 (2009).

154 *Id*. at 629.

155 *See* Interpace Corp. v. Lapp, Inc. 721 F.2d 460, 463 (3d Cir.1983)(*providing* 6 « lapp factors» test). *See also* Northland Ins. Companies v. Blaylock, 115 F. Supp. 2d 1108, 56 U.S.P.Q.2d (BNA) 1662 (D. Minn. 2000). AMF, Inc. v. Sleekraft Boats, 599 F.2d 341 (9th Cir. 1979).

156 Farley, at 627 (2009).

157 *Id*.

158 *Id*. at 628.

even if the services or products they offer are different from those offered by the objecting TLD operator.[159] Failing to ground the «confusingly similar» concept, by requiring that confusion is «likely,» may create a greater prohibition of new gTLDs. Considering whether it is possible for the existing gTLD <.asia> to prevent an application for a new gTLD like <.asians> the answer could depend on the standard applied. Under the standard in the AG, the answer is probably not. Considering the query on an objective basis, it is not likely that the average reasonable Internet user will be confused by the new gTLD. The existing gTLD <.asia> is based on a geographic area. The hypothetical <.asians> is targeted at a group of individuals.

However, if the standard in the attachment is used, and the only consideration is whether the potential gTLD is «confusingly similar,» it may be a closer call. The spelling of the gTLDs is similar, and if the confusion does not have to be likely, the DRSP could reach a different conclusion. If the DRSP relies solely on the attachment, the answer may vary further depending on the outside or «international standards» applied. Not all gTLDs that have similarities will be confusingly similar. However, requiring that the confusion be «likely» may provide new gTLDs with more flexibility in finding a viable name that does not infringe on the rights of others.

The AG provides some additional guidance for dispute resolution providers in determining names that are «likely to deceive or cause confusion.» By including an objective «average, reasonable Internet user» standard for determining «probable confusion,» ICANN has provided an avenue for DRSPs to avoid removing applications based solely on their similarity with existing gTLDs. The attachment to the AG does not contain the «reasonable Internet user» standard. However, what an «average, reasonable Internet user» looks like, on an objective basis, is not abundantly clear. The Internet is accessible the world over, extremely international, and its users vary considerably. Effectively creating and applying a standard that objectively defines the «average, reasonable Internet user» is therefore challenging. Like other objective «reasonable person» standards, it may be difficult to assign characteristics that adequately define what is «reasonable» or expected of an Internet user.

It remains to be seen how much of an impact, if any, the inconsistency between the AG and the attachment and the mixing of legal standards will have. The deviation between the AG and the attachment to the AG will be of little consequence in cases where the addition of a new gTLD would clearly be confusing (i.e. <.comm>).[160] On the other hand, if the attachment does allow

159 *Id.*

160 Assuming the gTLD is not removed in the string similarity review.

for significant divergence, the impact could affect the use of words or phrases as new gTLDs. However, as stated in the AG, it is subject to change. If a sharp divergence occurs, considerably limiting new gTLDs, ICANN would have the opportunity to adjust the attachment in future rounds. In addition to requiring that confusion be likely, consistent application of the «reasonable Internet user» standard may open opportunities for a greater number of gTLDs.

Considering the blending of legal standards, it is also unlikely that the discrepancy will stem the flow of available words or phrases suitable for new gTLDs. It has been noted that during UDRP proceedings, a «significant minority of panels assume that the meaning of the phrase 'confusingly similar' is identical with the traditional, 'likelihood of confusion' analysis in trademark law.»[161] Although the confusingly similar standard applied in the UDRP considers misuse of trademarks and the present objection evaluates confusion between applied for and existing gTLDs, the experience of new gTLDs could very well be similar. That is to say, even if the underlying basis of objection diverges, the experience of the UDRP may be a strong predictor of the experience with new gTLDs. Although the string confusion objection does not consider with trademarks directly, the drafters have borrowed some legal concepts and legal terms commonly found in trademark law. Even with the blending of legal standards in application of the UDRP, based on the limited studies available, parties have not regularly sought a *de novo* review in a court following the decision of a dispute resolution provider.[162]

If an existing gTLD operator is successful with their objection, the application for the confusingly similar gTLD will be denied. However, if the third party objecting is another applicant for a new gTLD, both applications will «be placed in a contention set,» and will be subject to the contention resolution procedure.[163] The situation where a party has the potential to make overlapping objections, based on their legal rights, including those arising out of trademark law, might also transpire.[164] For objections based on string confusion, the International Centre for Dispute Resolution (ICDR) will be the dispute resolution provider.[165] The applicable procedural rules are the ICDR Supplementary Procedures for the new gTLD program.[166]

161 Bettinger, at 1030 (2005).
162 Sorkin, at 35-55 (2001).
163 AG at 3.1.2.1. *See also* AG Module 4.
164 See Legal Rights Objection AG 3.5.2 discussed *Infra*.
165 AG at 3.1.3 Dispute Resolution Service Providers.
166 AG at 3.2 Filing Procedures.

2.5 Legal rights objection

In an attempt to protect legal rights holders, ICANN has provided trademark holders and others with the ability to object to new gTLDs that may infringe on their existing rights. To establish standing under the objection, the objecting party must have a legal right that will be infringed by the new gTLD.[167] Trademark holders, for example, will have the opportunity to object to an applied for gTLD that infringes on their trademark.[168] The objecting party may be the holder of a registered or unregistered trademark, or a service mark.[169] If the objector is successful, the new gTLD will not be issued. Module 3 provides that new gTLDs «must not infringe the existing legal rights of others that are recognized or enforceable under *generally accepted* and *internationally recognized* principles of law.»[170] In particular, the applied for gTLD must not take unfair advantage of the «distinctive character» or «reputation of» the objector's trademark or other legal rights.[171]

If an objection is based on a trademark right, the dispute resolution provider must consider a list of non-exclusive factors in reaching its determination.[172] The factors the DRSP will consider include general indicators such as likeness in appearance, sound, or meaning to the objector's mark.[173] In addition to traditional characteristics associated with trademark infringement, a dispute resolution provider must also evaluate additional abstract factors, including the intention of the applicant. For example, the dispute resolution provider may also consider «whether the applicant, at the time of application for the gTLD, had knowledge of the objector's mark, or could not have reasonably been unaware of that mark…»[174] The DRSP will also consider whether the proposed gTLDs use «would create *a likelihood of confusion* with the objector's mark.»[175] Additional factors such as the applicant's interest in the name and preparations made to use the gTLD, if granted, will also be taken

167 AG at 3.1.2.2 Legal Rights Objection (*including* either registered or unregistered trademarks).

168 *Id*. IGOs and specialized agencies including the UN may also meet the criteria.

169 *Id*.

170 AG at 3.52. Emphasis added.

171 *Id*.

172 AG at 3.52.

173 *Id*. at 3.52(1).

174 *Id*. at 3.52. (4).

175 *Id*. at 3.52.(6). Emphasis added. *See* Section 2.4. *See also* Komaitis, *Supra* note 150 at 560.

into account.[176] Additionally, any IP rights which correspond to the applied for gTLD will also be assessed.[177]

The legal rights objection has been criticized for being overly broad and providing greater protection to rights holders, particularly trademark holders, than exist in the offline world.[178] As argued by one author «…under this rule, the Cherokee Nation would be unable to use Cherokee as a gTLD because some automobile company is said to have prior rights under this policy.»[179] Protections granted under trademark law, are not the same in all jurisdictions. Although there are international treaties dealing with trademarks, there is no *per se* «generally accepted and internationally recognized» body of trademark law.[180] Trademark protections are not granted on a worldwide basis. Rather, they are provided for within a geographic area.[181] The lack of worldwide application allows for use of the same name or mark in multiple jurisdictions. The situation where a trademark is lawful in one geographic area, but infringes in another is not uncommon.[182] The same reality does not exist online. Like IP numbers, domain names must be unique. In the offline world, many commonly used words or phrases are able to obtain trademark protection because they are used in a distinctive manner. The classic example is the word «apple.» Although the term «apple» would not be distinctive to obtain a trademark for the fruit, it is distinctive for trademark purposes when being used to describe a brand of computers. Although globalization has certainly brought with it contention over the use of words as trademarks, there is still a measure of separation based on location offline.

Applying distinctions in geography and product class has been problematic on the Internet. In the case of *Prince plc v. Prince Sports Group Inc.*, two companies, one from the UK and the other from the US, sought the same domain name, www.prince.com.[183] Although the trademark name «Prince» could co-exist in the UK and US markets without incident, the DNS only allowed for one <www.prince.com>.[184] Although both parties seeking the name had a valid claim for the domain name, the resource was limited. Depending on how broadly the legal rights objection is construed, the gTLDs available to

176 *Id*. at 3.52. (5).
177 *Id*. at 3.52. (5-6).
178 Komaitis, at 49 (2010).
179 Farley, at 630 (2009).
180 *Id*. *See also* Prince plc v. Prince Sports Group Inc. [1998] FSR 21.
181 *Id*.
182 *Id*.
183 *Id*.
184 *Id*. Prince plc, the first register the domain name retained it despite the challenge by Prince Sports Group Inc.

applicants could be curtailed considerably. In the Prince case, the dispute was over a SLD, registered under the «non-distinctive» gTLD <.com>. However, under the right holders objection, provided for in the AG, if Prince plc applies for the gTLD <.prince> Prince Sports Group Inc., may be able to block the name from issuance. If the standard «infringes on the existing legal rights of others» is broadly construed, or the DRSP readily finds the «likelihood of confusion» test met, applicants could face a difficult road.[185] Based on the large number of trademark filings globally, it may be very difficult for an applicant to obtain a gTLD that is not in conflict with a trademark. This is particularly problematic when the phrases in the trademark are common. For example, the bank ING Direct has a trademark for «ING.»[186] Will use of «ING» in a new gTLD be enough to block it?

There are also cases where legal right holders will be unlikely to successfully block new gTLD applications. For example, if an association of heavy equipment manufacturers were seeking a new gTLD like <.diesel> it would not necessarily be disqualified as a result of the trademarked use of the word «diesel» by Diesel S.p.A, a clothing and fashion company.[187] Use of the word «diesel» in a gTLD would arguably infringe on the existing legal rights of Diesel S.p.A. However, when considering the non-exclusive factors in the AG, a DRSP would have to consider whether the gTLD <.diesel> would create «a likelihood of confusion» with the Diesel S.p.A.'s trademark.[188] Based on the required factors, it is unlikely that consumers visiting the website would confuse high fashion jeans and shoes with heavy trucks or other types of construction equipment. However, if the construction company began selling construction clothing, Diesel S.p.A, would have a better argument. If the hypothetical gTLD <.diesel> was granted and then began selling second level domain names in a manner inconsistent with its application, such as <www.jeans.DIESEL>, the trademark owner would have the opportunity to seek relief under the other Rights Protection Measures (RPMs) provided for in the AG. Specifically, the Post-delegation Dispute Resolution Procedure (PDDRP) would be pertinent.

It has been argued that confusion occurring with new gTLDs will be less problematic than it has been under the popular gTLD <.com>. Assuming the application would be approved; typosquatting with gTLDs like <.nkie> or a

185 AG at 3.52. (8).

186 McCarthy, Kieren, *Trademark lawyers to ICANN: close, but no cigar*, May 19, 2011. Available at http://news.dot-nxt.com/2011/05/19/ip-lobby-close-no-cigar (last visited: May, 27 2011).

187 http://en.wikipedia.org/wiki/Diesel_(brand)(last visited May, 27 2011). (*Selling* jeans and other fashion accessories).

188 AG at 3.52(6).

<.macdonalds> would be less attractive as the misspellings are less likely to be inadvertently visited by consumers.[189] Considering the cost of a new gTLD, it is also unlikely. Even at the second level domain space, typosquatting is unlikely to be as effective, unless the name is widely used.

The «existing legal rights objection,» on its face, appears to be a strong protection, particularly for trademark holders. The policy, if applied broadly, could significantly curtail options available to applicants. The boundaries of what should be considered a legal right are not entirely clear. Outside of the more traditionally protected groups, like trademark holders, module 3 also will also consider objections for an «IGO name or acronym.»[190] Will a second level domain name holder, without a trademark, have standing to object under the system? For example, can the sLD <www.house.com> limit a new gTLD like <.house>. If the answer were yes, it would seem that the ability to secure marketable gTLDs might be difficult. This also begs the question of whether owners of trademark rights are being provided with a monopoly on language in the expansion of the Internet. Could a more balanced approach have been taken?

All legal rights objections will be administered by the Arbitration and Mediation Center of the World Intellectual Property Organization (WIPO).[191] As a DRSP under the UDRP system, the WIPO dispute resolution panel has handled a high number of cases.[192] The WIPO track record also shows that panelists have decided for complainants in a high proportion of cases.[193] In one period, cases before a sole WIPO panelist were in favor of the complaining party 83% of the time.[194] However, the complaint success rate was much lower at 58% when a three-member panel was used.[195] The high rate of wins

189 Lipton, at 263 (Edward Elgar 2010). Clark, Christopher G., *The Truth in Domain Names Act of 2003 and a Preventative Measure to Combat Typo squatting*. Cornell Law Review, Vol. 89, No. 6, at 1476, (2004). Available at SSRN: http://ssrn.com/abstract=754524 (last visited September 30, 2011).

190 AG at 3.52.

191 AG3 at 3.1.3 Dispute Resolution Service Providers. During dispute resolution proceedings, the WIPO Rules for New gTLD Dispute Resolution are applicable. New gTLD DRP Art.2(e)(ii).

192 M. Mueller, «Rough Justice» (available at http://dcc.syr.edu/PDF/roughjustice.pdf)(last visited 23 September 2011).

193 Kaufmann-Kohler and Schultz, at 193 (2004).

194 *Id*.

195 Geist, Michael A., *Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP* (August 2001). Available at SSRN: http://ssrn.com/abstract=280630 or doi:10.2139/ssrn.280630. See also Bechtold, Stefan, *Governance in Namespaces*. Loyola of Los Angeles Law Review, Vol. 36, at 1261 (Spring 2003)(Discussing studies implicating bias of DRSPs). Available at SSRN: http://ssrn.com/abstract=413681 or doi:10.2139/ssrn.413681(last visited November 9, 2011).

for complainants is not, in and of itself, indicative of bias.[196] However, several factors, including the large amount of panelists also acting as practicing trademark lawyers, actively representing right holders, has raised some question of systemic bias.[197]

2.6 Limited public interest objection

The broadest available objection is the limited public interest objection. [198] The objection is essentially open, and allows any third-party to file an objection to a new gTLD.[199] Unlike the other objections in the dispute resolution section, there are no general standing requirements that must be met. The objection will be granted where the gTLD «is contrary to general principles of international law for morality and public order.»[200] Broad categories outlining the grounds for a legitimate public interest objection are provided for in the AG.[201] Although «general principles» are not specifically defined, a non-exhaustive list that includes a multitude of international instruments will be considered. Among others, the instruments include the Universal Declaration of Human Rights (UDHR) and the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW).[202]

At first blush, the objection appears to be extremely broad. A community as diverse as the one using the Internet does not have a single view on morality. However, despite the broad language of the standard for the objection, the AG narrows the categories for a dispute resolution provider to deny a gTLD in the AG. To be denied a gTLD pursuant to the objection, the gTLD must provide for incitement of violent lawless action, discrimination, or promotion of child pornography, along with other acts or subjects widely prohibited by «international instruments of law.»[203] Although some gTLDs may be contrary to «accepted legal norms relating to morality and public order,» it does not appear that the dispute resolution provider will be required to define morality based on the views of its most conservative members. The criteria to determine what is contrary to legal norms or morality will still require a measure of subjectivity in its application. However, by tying the determination firmly to principles

196 Zhao, at 178 (2005) (*Arguing* that charges of claimant bias remain unproven).
197 Kaufmann-Kohler and Schultz, at 193 (2004).
198 AG at 3.1.2.3 *Limited Public Interest Objection*.
199 AG discussion Draft at. 3.2.2.3.
200 *Id*.
201 AG at 3.4.3 (*Providing* examples of grounds for objection rather than an exhaustive list).
202 *Id*.
203 *Id*.

of international law, the DRSP will have a more objective basis for making the determination. Unlike the GAC Advice procedure discussed *infra*, simply offending a community with a gTLD such as <.jesus> or <.mohammed> is not necessarily sufficient for dismissal under the objection.[204] In the event of a «highly objectionable» application, a formal objection may also be filed by the Independent Objector (IO).[205]

Unlike other objections, those made in the public interest are subject to a summary or «quick look» procedure for dismissal.[206] The «quick look» procedure is designed to remove legitimate complaints from those that are frivolous, abusive, or «manifestly unfounded.»[207] Unlike most other sections of the guidebook, the drafters refer specifically to «manifestly ill-founded» as the most likely situation wherein an objection may be struck under the «quick look» procedure.[208] The International Center of Expertise of the International Chamber of Commerce will administer dispute resolution proceedings for objections based on limited public interest.[209] For dispute resolution proceedings taking place under the limited public interest objection, «three experts recognized as eminent jurists of international reputation» will be appointed.[210]

The limited public interest objection provides anyone with an interest in the Internet an opportunity to object to a new gTLD without a more tangible interest like a trademark. Creation of the objection provides those without specific commercial or other interest a voice in the gTLD process. Allowing this participation is consistent with the broad based, Multi-Stakeholder process championed by ICANN. Further, providing a foundation for evaluating objections, based on instruments of international law, provides greater credibility to a panel making decisions based on issues like morality. It remains to be seen how broadly the «quick look» procedure will be applied in rejecting applications. If applied too narrowly, and too few applications are considered legitimate, it could undermine the access it is intended to provide. Because an objection must be «frivolous and/or abusive» to be dismissed, the procedure is unlikely to be applied in a manner that undermines the value of the entire objection.[211]

204 AG at 3.2.5.
205 *Id*. at 3.2.5. The IO is limited to «(1) Public Interest objections and (2) Community objections.»
206 AG at 3.1.2.3 *Limited Public Interest Objection*. «An objection found to be manifestly unfounded and/or an abuse of the right to object may be dismissed at any time.»
207 *Id*.
208 AG at 3.2.2.3. FN3.
209 AG at 3.1.3 Dispute Resolution Service Providers.
210 AG at 3.3.4 Selection of Expert Panels.
211 AG at 2.2.2.3. Providing grounds for dismissing an application including morality.

2.7 Community Objection

The community objection provides «established institutions associated with clearly delineated communities» with standing to file an objection to a new gTLD.[212] To meet standing requirements, the community must show that it is an established one *and* that it serves a specific community. To determine whether an institution is «established» for purposes of the objection, the applicant guidebook provides a non-exhaustive list of factors to be considered.[213] Specifically, ICANN will consider how long the institution has existed and the public recognition of its existence.[214] Supporting evidence may include international validation or governmental registration by treaty. Institutions created for the sole purpose of objecting to new gTLDs will most likely be unable to meet standing requirements.

If the institutional requirements are met, the objecting institution must show that it has «an ongoing relationship with a clearly delineated community.»[215] The determination is based on multiple, non-exclusive factors, such as the «institutional purpose related to the benefit of the associated community…» In determining whether standing is applicable, ICANN may also consider additional factors not enumerated in the AG.[216] The International Center of Expertise of the International Chamber of Commerce will administer dispute resolution proceedings for objections based on community objections.[217] One expert will be appointed to administer dispute resolution proceedings occurring under the community objection.[218]

2.8 GAC Advice on New gTLDs

After much of the dispute resolution procedures had been drafted, ICANN added a new avenue for governments, through the Governmental Advisory Committee (GAC), to oppose or provide «advice» on any new gTLD application.[219] The advice procedure will allow governments to address applicati-

212 AG at 3.1.2.4. *See also* AG at 3.2.5. The IO also has standing to make «Community objections.»
213 *Id*.
214 *Id*.
215 *Id*.
216 *Id*.
217 AG at 3.1.3 Dispute Resolution Service Providers.
218 AG at 3.3.4 Selection of Expert Panels.
219 AG discussion Draft at 3.1. GAC Advice on New gTLDs. The Governmental Advisory Committee (GAC) «was formed to consider and provide advice on the activities of ICANN as they relate to the concerns of governments…» *Id*.

ons they identify «to be problematic.»[220] The new GAC procedure was added following an ongoing debate between members of the GAC and the ICANN board on the role of governments in the new gTLD process.[221] At the outset of this discussion, it is worth noting that the GAC procedure, as provided for in the AG, will likely undergo changes. The most current AG provides that the GAC «has expressed the intention to develop a standard vocabulary and set of rules for use in providing its advice…» [222] The section states that it «might be updated» to reflect the changes provided by the GAC.[223] Although there has been some discussion by the GAC indicating how procedures such as GAC «consensus,» may ultimately be defined, definitions have not been finalized.[224]

Although the specific GAC «advice» procedure that was ultimately adopted may not have been included in early drafts, it was likely an important step procuring approval of the AG.[225] The GAC has played an increasingly important role in gTLD name policy since 2002.[226] For example, the GAC, in conjunction with the US government and other groups, was central to blocking the <.xxx> domain name after its initial ICANN approval in 2005.[227] Regarding the new gTLD program, the GAC has requested considerable authority in determining acceptable domain names. In 2007, the GAC requested a procedure for blocking new domain names, at no cost, which would be «on demand for governments.»[228]

Although some issues regarding the GAC's role have been resolved, issues relating to the protection of trademarks and sensitive names have continued to be a significant point of conflict. In addition to opposition provided by the GAC, the US government submitted a letter of opinion on the matter. The US suggestion was to remove the *Limited Public Interest Objection* and provide for a review by the GAC in its place. The US position criticized the current public interest standard as problematic arguing there are no «generally ac-

220 AG. 3.1.
221 For documents including scorecards see. http://gac.icann.org/ (last visited May 18, 2011).
222 AG. 3.1.
223 *Id*.
224 Available at: http://www.icann.org/en/committees/board-gac-2009/board-gac-jwg-final-report-19jun11-en.pdf (last visited September, 27 2011).
225 Papac, Krista, *ICANN Successfully Tiptoes Through Political Minefield With New TLD Applicant Guidebook*, Circle ID, (May 12, 2011). Available at: http://www.circleid.com/posts/20110512_icann_tiptoes_through_political_minefield_new_tlds/ (last visited November 10, 2011).
226 Weinberg, at 6-7 (2011).
227 *Id*. As stated *Supra*, the <.xxx> gTLD has since been approved.
228 *Id*. (*Citing* GAC Principles Regarding New gTLDs §§ 2.1, 2.2, 2.7 (March 28, 2007) Available at: http://gac.icann.org/system/files/gTLD_principles_0.pdf (last visited May, 14 2011).

cepted legal norms,» as provided for in the objection. Additionally, the US government argued that allowing a private expert to make determinations of morality and legal norms was «contrary to the sovereign right of governments to interpret and apply principles of international law on a country-by-country basis.»[229]

Following discussion with the GAC, the module 3 advice or objection mechanism was adopted. The purpose of the GAC objection is to allow governments to object to new gTLDs «that potentially violate national law *or* raise sensitivities.»[230] From a procedural point of view, the GAC advice period functions much like the other objections or challenges provided in module 3. Any advice presented by the GAC to ICANN must take place within the objection filing period.[231] If the GAC objects to a gTLD, the applicant will have 21 days to respond to ICANN after it receives notice of the objection. A major procedural difference from other objections is how the complaint will be administered. Unlike other objections in this section, an independent dispute resolution provider will not consider GAC objections. [232] Rather, the ICANN board will play the role of DRSP. The ICANN board has the option to consult with independent experts, but consultation is not required.[233]

From a substantive point of view, the new procedure provides very little guidance as to its application. Weight or deference given to the GAC advice will also take different forms, depending on whether there is «consensus» advice from the GAC, stating that an application should not proceed.[234] In the current AG, what constitutes GAC «consensus» remains undefined.[235] Essentially, if the GAC advises ICANN that a given application should not proceed, it will create «a strong presumption for ICANN that the application should not be approved.»[236] However, the presumption is not irrefutable.[237] If ICANN approves an application despite an objection from the GAC, ICANN must provide a rationale for its decision.[238]

If there is no «consensus» that an application should not proceed, but «some governments» are concerned about an application, the concern will be taken

229 USG submission to the GAC Scorecard re New gTLDs. Objection procedures.
230 AG at 3.1. GAC Advice on New gTLDs.
231 *Id*.
232 *Id*. III.
233 AG at 3.1.
234 AG at 3.1(I-III).
235 *Id*. FN 1 (stating «The GAC will clarify the basis on which consensus advice is developed.»).
236 *Id*. at I.
237 *Id*.
238 *Id*.

into consideration by the ICANN board.[239] The concern by the governments will be taken seriously, however, no presumption will be formed.[240] The GAC may also advise ICANN that an application should not proceed unless remediated.[241] It is unclear what sort of agreement much be reached by the GAC members before they may «advise» remediated.[242] In any event, if remediation is advised, a strong presumption that remediation is necessary will occur before the application is accepted.[243] The line between what is «remediation» or a generally prohibited «amendment» to an application is not entirely clear. However, material amendments «are generally prohibited.»[244] If no clear method for remediation exists, such as securing government approval for use of the name of a capital city, the application will not move forward.[245] As a result, the effect of GAC suggested remediation might be a difficult barrier to overcome for gTLD applicants. In some respects, the numeration advice will have a similar effect to a «consensus objection,» without requiring a «consensus» position by the GAC.

The new objection has been criticized as vague and providing one group, the GAC, with too much influence in the gTLD process. Critics have particularly argued that providing governments with too much power, via a government veto or other procedural mechanism, could have negative consequences for freedom on the Internet. For one, it could also lead to much broader censorship on the Internet. As stated by Milton Mueller, «[t]he ICANN process has spent years trying to ensure that only applications that involve words contrary to general principles of international law will be vetoed.»[246] In Mueller's review of a GAC veto, he uses the example of the potential domain name <.gay> as a gTLD that is important to a community, but may be vulnerable under the new objection.[247] Muller maintains that based on conversations with conservative governments within the GAC, there is objection to a <.gay> domain name.[248] Under the proposed GAC objection, does the domain name <.gay> potentially

239 AG at 3.1(II).
240 *Id*.
241 *Id*.
242 *Id*. It is unclear if «advises… that an application should not proceed unless remediated» is the same as «provides advice that indicates that some governments are concerned» is sufficient for a recommendation.
243 AG at 3.1(III).
244 *Id*.
245 *Id*.
246 Muller, Milton, *The US Commerce Dept position paper for the ICANN Board negotiations*, Internet Governance Project., January 29, 2011. Available at: http://blog.internetgovernance.org/blog/_archives/2011/1/29/4737705.html (last visited November 11, 2011).
247 *Id*.
248 *Id*.

«raise sensitivities» to an extent that it may be blocked? The disjunctive use of «or» indicates that the domain name does not have to be illegal in a jurisdiction, but simply «sensitive.» What constitutes sensitive information is unclear.[249] Although domain names like <.jesus> or <.mohammed> may be likely candidates for raising sensitivities, it is unclear whether they could be blocked under this objection. Will there emerge a system where votes for trademark protection are traded for votes to block sensitive names?

The counter argument to complaints about the breadth of the new GAC objection is that the policy contains checks on the power granted. If consensus is not reached, the presumption will not apply. Arguably, it is unlikely that a handful of conservative countries with strict religious codes or blasphemy laws will have the ability to block a significant number of new gTLDs. Even if an application is objected to, with GAC consensus, the ICANN board will have the opportunity to accept or reject the advice.[250] As a result, ICANN will remain in a position to rebut a presumption based on GAC advice. Applicants that are subject to objections will have options.[251] First, the applicant may opt to settle the dispute, which will result in withdrawal of either the application or the objection.[252] Second, the applicant can file a response to the objection, potentially removing government opposition.[253]

Unlike the majority of the AG, it appears the GAC objection is still being worked out. Although the GAC advice procedure may have been a politically necessary step for the adoption of the AG, it has also raised concerns regarding the freedom of speech associated with new gTLDs. Allowing the advice procedure to be applied broadly could have an effect on the gTLDs available. In addition to <.gay>, will names like <.wine> or <.beer> be limited by the more conservative members of the constituency? A clearer finished procedure, providing clearer definitions of terms like consensus, may have reduced anxiety over the procedure.

3 Conclusion

The current round of gTLD expansion has made substantial changes and great improvements from earlier rounds. The current expansion has been planned, debated, and allowed many interested parties to provide input on the process. Unlike earlier rounds, where applications were denied based on whether they

249 http://www.icann.org/en/topics/new-gtlds/gac-objections-sensitive-strings-15apr11-en.pdf.
250 AG at 3.1.
251 AG at 3.1.4.
252 *Id.*
253 *Id.*

could be easily pronounced by members of the ICANN board, the current process has taken a much more open and systematic approach in the planning of and drafting of the AG. By removing the mystery of earlier rounds, and setting out a more balanced system, the new rounds of dispute resolution further the goals of the Multi-Stakeholder model.

There are aspects of the guidebook that could have been approached differently. Mixing legal standards in the legal rights and string confusion objections may be problematic, particularly if their application by a DRSP deviates substantially from the standards set out in the AG. Charges that holders of trademarks were given a higher priority in the process are not without some merit. Substantial efforts have been placed on trademark protection in accepting new gTLD applications and that heightened level of protection continues after gTLDs are issued. In my opinion, the danger brought by this policy is not that trademarks will be run over in the process. Rather, it is that the systems designed to protect them will limit available gTLDs to an extent that it will be difficult to obtain names that are commercially viable.