Digitalisering och personlig integritet: En systematisk kunskapsöversikt

Rosengren, Calle; Svensson, Måns; Åström, Fredrik

2016

Rapport från Rättssociologiska institutionen och Lunds universitets internetinstitut 2016

Digitalisering och personlig integritet

En systematisk kunskapsöversikt

Digitalisering och personlig integritet

En systematisk kunskapsöverikt

Framtagen av Lunds universitet i samarbete mellan Lunds universitets internetinstitut, Rättssociologiska institutionen och Universitetsbiblioteket

Projektledare

Måns Svensson, docent i rättssociologi

Författare

Calle Rosengren
Måns Svensson
Fredrik Åström

Innehållsförteckning

Sammanfattning

Forskningsområdet *digitalisering och personlig integritet*, så som det definierats och avgränsats (framförallt genom val av söksträngar), inom ramen för den här kunskapsöversikten, är under tillväxt. Föreliggande studie har begränsats till engelskspråkiga artiklar publicerade i vetenskapliga peer-review-granskade tidsskrifter. Under de senaste 10 åren har antalet vetenskapliga artiklar per år inom området mer än femdubblats. Exempelvis ger en sökning i forskningsdatabasen WEB OF SCIENCE avseende 2006 13 träffar medan en identisk sökning avseende 2014 ger 72 träffar.

I den här systematiska kunskapsöversikten har två typer av undersökningar genomförts. För det första en bibliometrisk analys som syftar till att, på en statistisk analytisk nivå, skapa en övergripande bild av hur forskningen på området ser ut. För det andra en systematisk litteraturstudie där relevanta vetenskapliga artiklar har identiferats, analyserats innehållsmässigt och kategoriserats.

Den bibliometriska analysen visar att det föreligger en tämligen strikt uppdelning av forskningen om digitalisering och personlig integritet mellan huvudsakligen tre vetenskapliga fält. Det vill säga att kommunikationen mellan fälten (i termer av att referera och citera varandras arbeten) är förhållandevis begränsad. Forskningsfälten kan beskrivas som (a) ett tekniskt fält som i hög grad handlar om systemutveckling, (b) ett juridiskt fält med fokus på frågor om lagstiftat skydd av personlig integritet, samt (c) ett mer samhälls- och beteendevetenskapligt orienterat fält som bland annat samlar informatik, psykologi, sociologi, statsvetenskap och marketing- och managementforskning.

Den systematiska litteraturöversikten, som baseras på en genomläsning av samtliga ingående artiklar, visade att det även inom de olika vetenskapliga disciplinerna saknas tydliga gemensamma begreppsapparater och gemensam syn på metod. Dock kan man se ett antal olika områden (eller forskningsfokus) vilka är frekvent återkommande. De fem dominerande områdena är: (a) teknik, (b) lagstiftning, (c) stat, (d) teori och (e) arbetsliv.

Dessutom kan man i forskningen identifiera olika förhållningssätt i förhållande till digitalisering och personlig integritet. För det första *som ett problem* (eller kanske snarare utmaning) som går att hantera med hjälp av ny, bättre och mer integritetskänslig teknik. För det andra *som en möjlighet* att genom nyttiggörandet av potentiellt integritetskänslig data kunna verka för goda värden såsom förbättrad hälsa. För det tredje *som ett hot* mot medborgare och anställda. Och till sist som *en utbytesrelation* mellan nytta och risk, exempelvis avseende staters behov av information för att förebygga hot och medborgares rätt till integritet.

Slående är att det saknas tillräcklig kunskap avseende relationen mellan övervakning i det digitala och eventuella beteendeförändringar i samhället. Olika studier pekar på risker för att bristande respekt för den privata integriteten kan leda till minskat internetanvändande och minskat politiskt engagemang (åtminstonde på nätet). Dock saknas det ännu empiriska bevis för att så skulle vara fallet.

1. Inledning

Föreliggande kunskapsöverikt har genomförts av Lunds universitet på uppdrag (reglerat i avtal 2015-04-23) av Integritetskommittén (Ju 2014:09). Integritetskommitténs arbete preciseras genom direktiv 2014:65 som anger att den parlamentariskt sammansatta kommittén skall: Utifrån ett individperspektiv kartlägga och analysera sådana faktiska och potentiella risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik i såväl privat som offentlig verksamhet samt inom ramen för detta arbete följa upp effekterna i lagstiftningsarbetet av förstärkningen av grundlagsskyddet för den personliga integriteten som genomfördes 2011, och med beaktande av samhälls- och teknikutvecklingen i stort och mot bakgrund av slutsatserna av kartläggnings- och analysuppdraget, följa upp betänkandet Skyddet för den personliga integriteten (SOU 2008:3) när det gäller behovet av att inrätta ett integritetsskyddsråd och särskilt överväga om de uppgifter som ett sådant råd i så fall bör ges lämpligen kan fullgöras av en befintlig myndighet, samt föreslå nöd- vändiga författningsändringar.

Det uppdrag från Integritetskommittén som ligger till grund för den här kunskapsöversikten har formulerats enligt följande: I kunskapsöversikten skall framgå vilka studier av intresse som har gjorts både här i Sverige och i omvärlden när det gäller frågan om hur individer, grupper och samhällen påverkas av att vara övervakade, tro sig vara övervakade, eller av att de kan bli föremål för övervakning (även om de inte blir det). Detsamma gäller studier om hur människor, inklusive organisationer och företag, har påverkats av de möjligheter som nu finns att aktivt övervaka/kontrollera andra. Med påverkan avses hur inställning/synsätt och beteende förändras. Av kunskapsöversikten skall vidare framgå om studier har gjorts inom särskilda områden, exempelvis om patienters inställning och hur de påverkas, eller om arbetsgivares beteende påverkats, både i samband med nyrekrytering och beträffande sina anställda. Om eventuella skillnader i synsätt och beteende mellan olika kön har behandlats i någon studie skall det lyftas fram, liksom skillnader mellan olika åldrar. Det är t.ex. av intresse om det finns studier gällande barn som växer upp i den digitala miljön.

Metoden som använts för uppdraget är den vetenskapliga systematiska litteraturstudien samt bibliografisk analys. Sökningar på svenska gav ytterst få träffar, varför den delen av uppdraget lämnas därhän. Fokus ligger på vetenskapliga peer-review-granskade artiklar på engelska.

2. Metod

I grunden är den systematiska kunskapsöversikten en forskningsstudie som samlar in, analyserar och sammanställer studier inom ett visst område (eller utifrån en specifik frågeställning). Således kan den systematiska kunskapsöversikten beskrivas som ett sätt att sammanställa kunskapsläget inom ett visst område genom en strukturerad och systematisk insamling och granskning av vetenskapliga studier. Insamlingen av olika studier sker oftast genom sökning efter vetenskapliga publikationer i databaser (t ex EBSCO eller Web of Science) och styrs då av relevanta sökord. Genom att metod, utgångspunkter och sökkriterier synliggörs säkras transparens och möjligheten att replikera studien ökar. Inom ramen för föreliggande kunskapsöversikt används de tre steg som Tranfield et al. (2003) beskriver i *Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review* (2003): (a) Planering; (b) söka, identifiera och organisera publikationer; samt (c) extrahera och värdera. Vid varje steg krävs det ett antal överväganden vad gäller såväl sökkriterier som frågor rörande vilka publikationer som ska inkluderas respektive exkluderas. Nedan redovisas hur Transfields (et al.) metod har applicerats inom ramen för föreliggande studie.

(a) Planering av studien

Kunskapsöversikten fokuserar frågor som rör digitalisering och personlig integritet. Av särskilt intresse är övervakning genom det digitala mediet samt dess eventuella konsekvenser för attityder, beteende och integritet/privatliv. Om möjligt skall studien kunna belysa specifika gruppers förutsättninar (exempelvis baserat på ålder och kön), samt identifiera tematiska områden för vilka frågeställningen är relevant.

Viktiga avgränsningar utgörs av det faktum att det systematiska sökandet efter vetenskapliga publikationer i den här studien begränsas till artiklar i vetenskapliga tidsskrifter vilka är skrivna på engelska. De publikationer inom området som finns på svenska är i regel inte vetenskapliga i den meningen att de inte är peer-review-granskade och därmed inte har genomgått den process som garanterar vetenskaplig kvalitet. Det här gäller i synnerhet för artiklar, men i hög utsträckning även för böcker och rapporter. Ett viktigt undantag utgörs av doktorsavhandlingar vilka uppfyller vetenskapliga krav, men som ändå faller utanför begränsningarna för den här studien. Med detta sagt är det viktigt att understryka att relevant kunskap om specifka svenska förhållanden kan återfinnas i så kallad grålitteratur (ej vetenskapligt granskade rapporter, myndighetstryck, fackböcker etc.) som inte redovisas här.

(b) Söka, identifiera och organisera artiklar

Digitaliseringen av samhället har utifrån ett integritetsperspektiv inneburit stora utmaningar som rör ett flertal olika forskningsfält. De frågor som hanteras rör relationer mellan stat och medborgare, mellan konsument och företag, mellan arbetsgivare och arbetstagare och även mellan enskilda individier. Tekniken erbjuder nya möjligheter att kommunicera och serva kunder och medborgare, men samtidigt oanade möjligheter att kartlägga individers åsikter och beteende. Ambitionenen med denna kunskapsöversikt är att skapa en så bred bild som

möjligt av var forskningen avseende digitalisering, integritet och påverkan på människor står.

För denna systematiska kunskapsöversikt bedömdes att det framförallt var två databaser som var lämpliga och det är SCOPUS samt Web of Science (Core collection). SCOPUS, som ägs av Elsevier, indexeras ca 22 000 vetenskapliga tidskrifter och har en bred täckning vad gäller olika discipliner och ämnen. Web of Science är en databas (inkluderande bland annat 12 000 vetenskapliga tidskrifter av högsta kvalitet) publicerad av Thompson Reuters som förtecknar internationell forskningslitteratur, framför allt tidsskriftsartiklar på engelska. Fördelen med denna databas är att informationen är innehållsmässigt rik och möjliggör långtgående bibliometriska analyser.

(c) Extrahera och värdera materialet

I syfte att ge en så heltäckande bild som möjligt över kunskapsläget har vi för denna systematiska kunskapsöversikt valt att genomföra såväl en bibliometrisk analys som en systematisk litteraturöversikt. En bibliometrisk analys handlar i grunden om att, med hjälp av statistiska analyser av texters och textsamlingars egenskaper, skapa en bild av inom villka forskningsfält som en företeelse (eller fenomen) studeras samt i vilken utsträckning som dessa fält relaterar sina resultat till andra fälts studier av samma företeelse. En systematisk litteraturöversikt är i princip en sammanställning av relevant litteratur inom ett specifikt område. Insamligen bygger på en noggrann och systematisk metod för litteratursökning. Till skillnad från, och som komplement till den bibliometriska analysen, innehåller denna metod även en kvalitativ komponent i det att litteraturen som söks ut även läses och värderas.

3. Resultat

Bibliometrisk analys

För att ge en överblick över vilka forskningsfält som behandlar frågor om personlig integritet i digitala sammanhang, samt vilka frågor denna forskning behandlar, genomfördes bibliometriska analyser av forskningslitteraturen.

De bibliometriska analyserna är baserade på sökningar i Web of Science-databaserna (WoS), en samling databaser som framför allt indexerar artiklar på engelska publicerade i internationella vetenskapliga tidskrifter. Nackdelen med att använda dessa databaser är att den forskningslitteratur som publiceras på andra språk och/eller i andra dokumenttyper (t.ex. böcker) inte blir tillgänglig. Fördelen är att WoS, förutom vanliga former av metadata som t.ex. författare och titel, också indexerar referenserna i de vetenskapliga texterna, vilket gör det möjligt att göra olika typer av citerings- och begreppsanalyser.

För att identifiera den forskningslitteratur i WoS som behandlar frågor om personlig integritet och övervakning i digitala sammanhang användes följande söksträng i ”topic”-fältet (som täcker begrepp som förekommer i titel, abstrakt och nyckelord): (Surveill*) AND (online* OR digital* OR Internet*) AND (behav* OR attitud* OR privac* OR "norms"). Vidare begränsades sökningen dels i tid, till perioden 2005-2015, dels ifråga om dokumenttyp, där endast original- och översiktsartiklar inkluderades i sökningen (Figur 1).

> You searched for: TOPIC: ((Surveill*) AND (online* OR digital* OR Internet*) AND (behav* OR attitud* OR privac* OR "norms"))
> Refined by: DOCUMENT TYPES: (ARTICLE OR REVIEW)
> Timespan: 2005-2015.
> Indexes: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.
> Results: 506

Figur 1. Söksträng för den Web of Science-sökning som bildar bas för datainsamling för de bibliometriska analyserna.

Sökningen resulterade i 506 artiklar, men i och med att begrepp som t.ex. ”surveillance”, även när de kopplas till begrepp som hanterar digitala sammanhang eller frågor om beteende, fångar in vetenskapliga artiklar som inte är relevanta för det sammanhang som analyseras här. Exempel på detta är ”surveillance” som ett viktigt begrepp inom epidemiologin, bevakning av patienter i samband med operationer eller hälso- och riskbeteenden vid t.ex. vård av missbrukare. Det rör sig alltså mer om övervakning som en vårdmetod snarare än säkerhets- och integritetsfrågor i samband med hantering av patientinformation. För att i så stor utsträckning undvika irrelevant litteratur gjordes ytterligare en begränsning där ett 50-tal WoS-kategorier (kategorier som beskriver tidskrifters huvudsakliga

ämnesinnehåll) exkluderades ur sökningen, vilket resulterade i en ny uppsättning omfattande 311 artiklar (Figur 2).

Refined by: [excluding] WEB OF SCIENCE CATEGORIES: (RESPIRATORY SYSTEM OR INFECTIOUS DISEASES OR RADIOLOGY NUCLEAR MEDICINE MEDICAL IMAGING OR PHARMACOLOGY PHARMACY OR ECOLOGY OR PERIPHERAL VASCULAR DISEASE OR SOCIAL SCIENCES BIOMEDICAL OR TROPICAL MEDICINE OR PARASITOLOGY OR MEDICINE GENERAL INTERNAL OR PSYCHOLOGY CLINICAL OR GENETICS HEREDITY OR ENDOCRINOLOGY METABOLISM OR FOOD SCIENCE TECHNOLOGY OR DERMATOLOGY OR ONCOLOGY OR VETERINARY SCIENCES OR IMMUNOLOGY OR TOXICOLOGY OR ENGINEERING BIOMEDICAL OR SURGERY OR CLINICAL NEUROLOGY OR PEDIATRICS OR BIODIVERSITY CONSERVATION OR PATHOLOGY OR BIOCHEMISTRY MOLECULAR BIOLOGY OR SUBSTANCE ABUSE OR OBSTETRICS GYNECOLOGY OR MEDICINE RESEARCH EXPERIMENTAL OR AGRICULTURE MULTIDISCIPLINARY OR ERGONOMICS OR REHABILITATION OR ZOOLOGY OR VIROLOGY OR GASTROENTEROLOGY HEPATOLOGY OR UROLOGY NEPHROLOGY OR OPHTHALMOLOGY OR OCEANOGRAPHY OR NUCLEAR SCIENCE TECHNOLOGY OR METEOROLOGY ATMOSPHERIC SCIENCES OR ENVIRONMENTAL SCIENCES OR MARINE FRESHWATER BIOLOGY OR LIMNOLOGY OR MATHEMATICAL COMPUTATIONAL BIOLOGY OR FISHERIES OR ENTOMOLOGY OR EMERGENCY MEDICINE OR ELECTROCHEMISTRY OR CHEMISTRY ANALYTICAL OR CARDIAC CARDIOVASCULAR SYSTEMS OR BIOCHEMICAL RESEARCH METHODS)
Results: 311

Figur 2. Forskningsfält exkluderade ur Web of Science-sökningen.

Avgränsningen resulterade i en mer begränsad dokumentmängd med färre irrelevanta dokument. Men ser man till de enskilda artiklar som fångas in (exemplifierat nedan av de tio senast indexerade dokumenten funna i sökningen), kan man se att det fortfarande finns artiklar som ligger vid sidan om fokus för denna litteraturöversikt. Att göra ytterligare avgränsningar i sökningen i WoS är svårt eftersom man då riskerar att exkludera allt för mycket litteratur som skulle kunna vara relevant.

Brown, S. 2015) Moving elite athletes forward: examining the status of secondary school elite athlete programmes and available post-school options. Phys Ed Sport Ped, 20(4), 442-458.

Hall, EC. & Willett, RM. (2015). Online Convex Optimization in Dynamic Environments. IEEE J Select Topics Signal Proc, 9(4), 647-662.

Ramsey, LR. & Hoyt, T. (2015). The Object of Desire: How Being Objectified Creates Sexual Pressure for Women in Heterosexual Relationships. Psych Women Quart, 39(2), 151-170.

Park, MS. Et.al. (2015). Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. Psych & Marketing, 32(6), 601-610.

El Maadi, A. & Djouadi, MS. (2015). Using a Light DBSCAN Algorithm for Visual Surveillance of Crowded Traffic Scenes. IETE J Res, 61(39, 308-320.

Lukacs, V & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. Inform Commun & Soc, 18(5), 492-508.

Cover, AY. (2015). Corporate Avatars and the Erosion of the Populist Fourth Amendment. Iowa Law Rev, 100(4), 1441-1502.

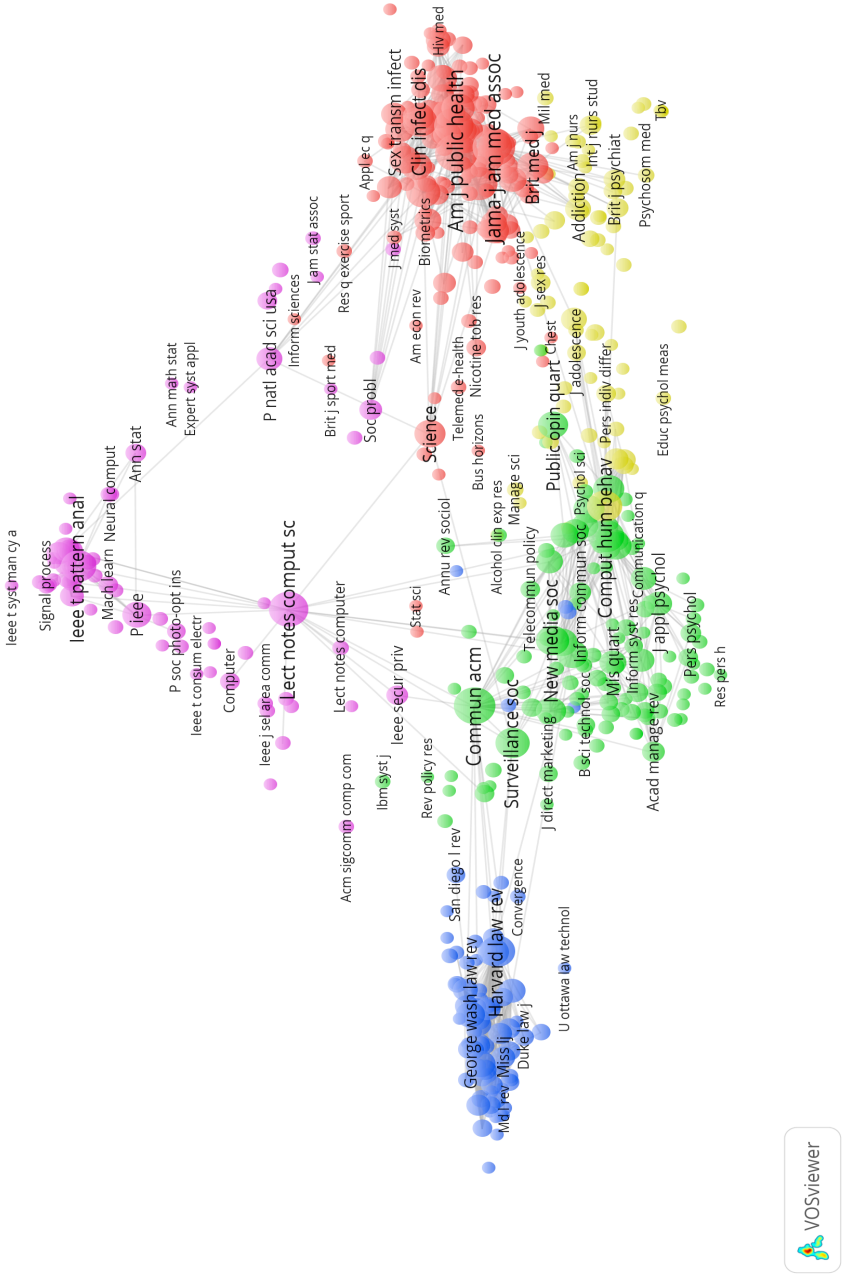
Roberts, A. (2015). Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications. Mod Law Rev, 78(3), 535-548.
Cavazos-Rehg, PA. Et al. (2015). Monitoring of non-cigarette tobacco use using Google Trends. Tobacco Control, 24(3), 249-255.
Lee, HK. & Choo, HJ. (2015). Daily outfit satisfaction: the effects of self and others' evaluation on satisfaction with what I wear today. Int J Consum Stud, 39(3), 261-268.

Figur 3. Exempel på heterogenitet i artiklar funna i Web of Science-sökningen. De tio senast indexerade artiklar i dokumentsetet.

Informationen från WoS om de återstående 311 artiklarna laddades ner. För att bearbeta data användes Bibexcel (https://bibliometrie.univie.ac.at/bibexcel/), ett program för bibliometriska analyser där man bl.a. kan renodla informationen från WoS för att analysera specifika fält, t.ex. titel, författare eller citerade referenser; men också delar av specifika fält, t.ex. tidskriftsnamnen för citerade referenser. De data som framtagits genom Bibexcel användes sedan vidare i VOSviewer, version 1.6, (http://www.vosviewer.com/), ett program för utförande och visualisering av bibliometriska nätverksanalyser.

Analys av forskningsfält
För att identifiera vilka forskningsfält som studerar frågor om övervakning och personlig integritet valdes co-citeringsanalys på tidskriftsnivå. Tanken är att man studerar den litteratur som forskningen använt genom att analysera referenslistorna och antar att artiklar eller – i detta fall – tidskrifter som citeras tillsammans har ett ämnesmässigt samband. Om man gör dessa analyser baserat på hundratals eller tusentals artiklar med 10 000- eller 100 000-tals referenser, så bildar samförekommande citerade artiklar eller tidskrifter kluster som representerar olika forskningsinriktningar eller forskningsfält.

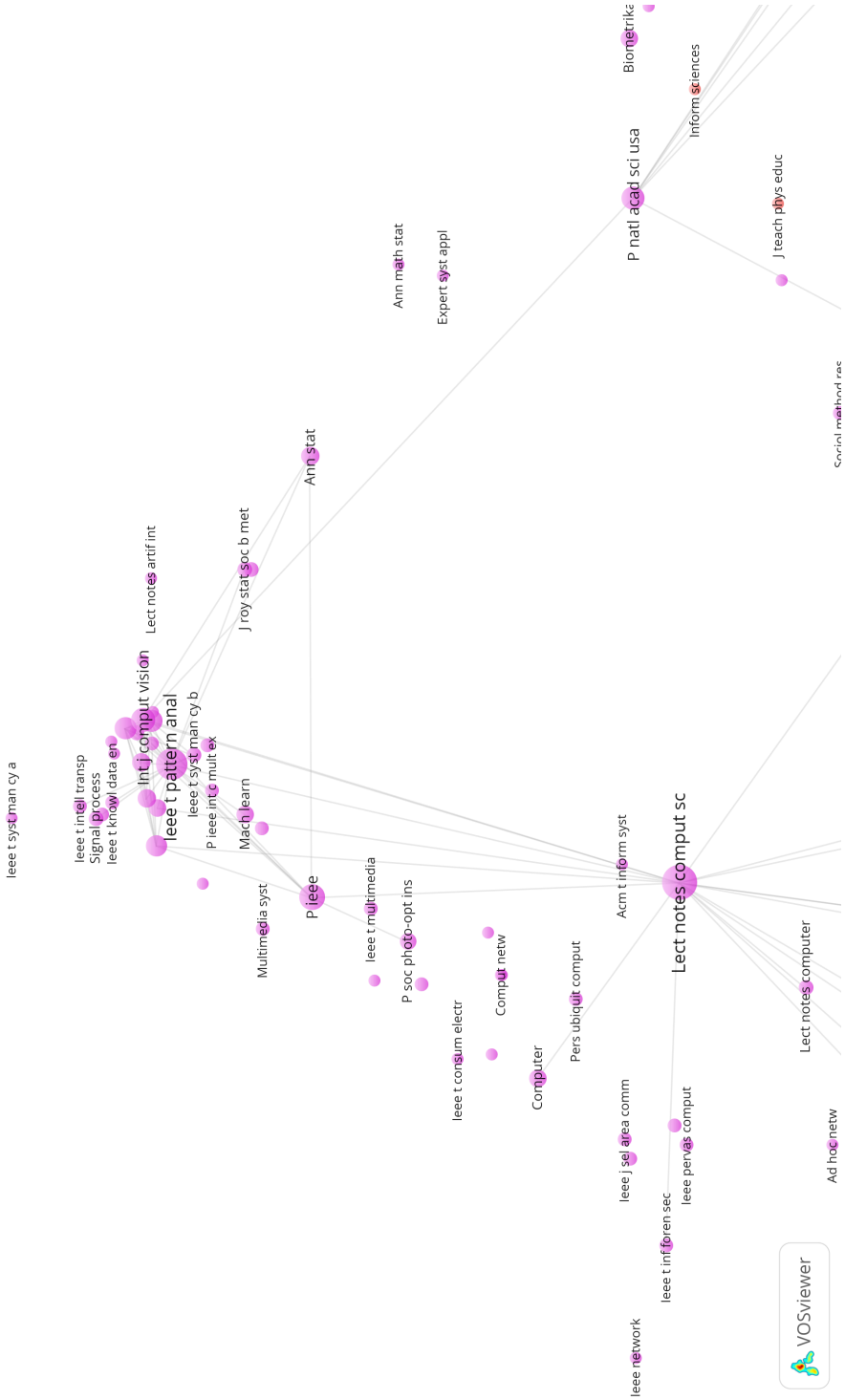
Följande analys bygger alltså på hur ofta citerade tidskrifter förekommer tillsammans i referenslistorna för de artiklar som identifierades i sökningen efter litteratur om integritet och digital övervakning. Kartan är baserad på analyser av de 500 mest citerade tidskrifterna. På kartan ser vi dels vilka tidskrifter som citeras ofta – representerat av storlek på noder och tidskriftstitel – dels hur tidskrifterna placeras i förhållande till varandra – baserat på hur ofta de citeras tillsammans. Citeras de ofta tillsammans placeras de närmare varandra, citeras de tillsammans mer sällan hamnar de längre ifrån varandra. Förutom samförekomster representerade genom närhet på kartan görs det också en klustringsanalys, som identifierar statistiska samband, också baserat på samförekomster. Dessa kluster representeras av olika färger. Vidare kompletteras analysen också med linjer som representerar starkare samband (mer än 1 000 co-citeringslänkar), vilket gör att man kan se i vilken utsträckning de olika klustren länkar tillsammans och – i förlängningen – i vilken utsträckning olika forskningsfält kommunicerar med varandra (se nedan).



Figur 4. Co-citerade tidskrifter.

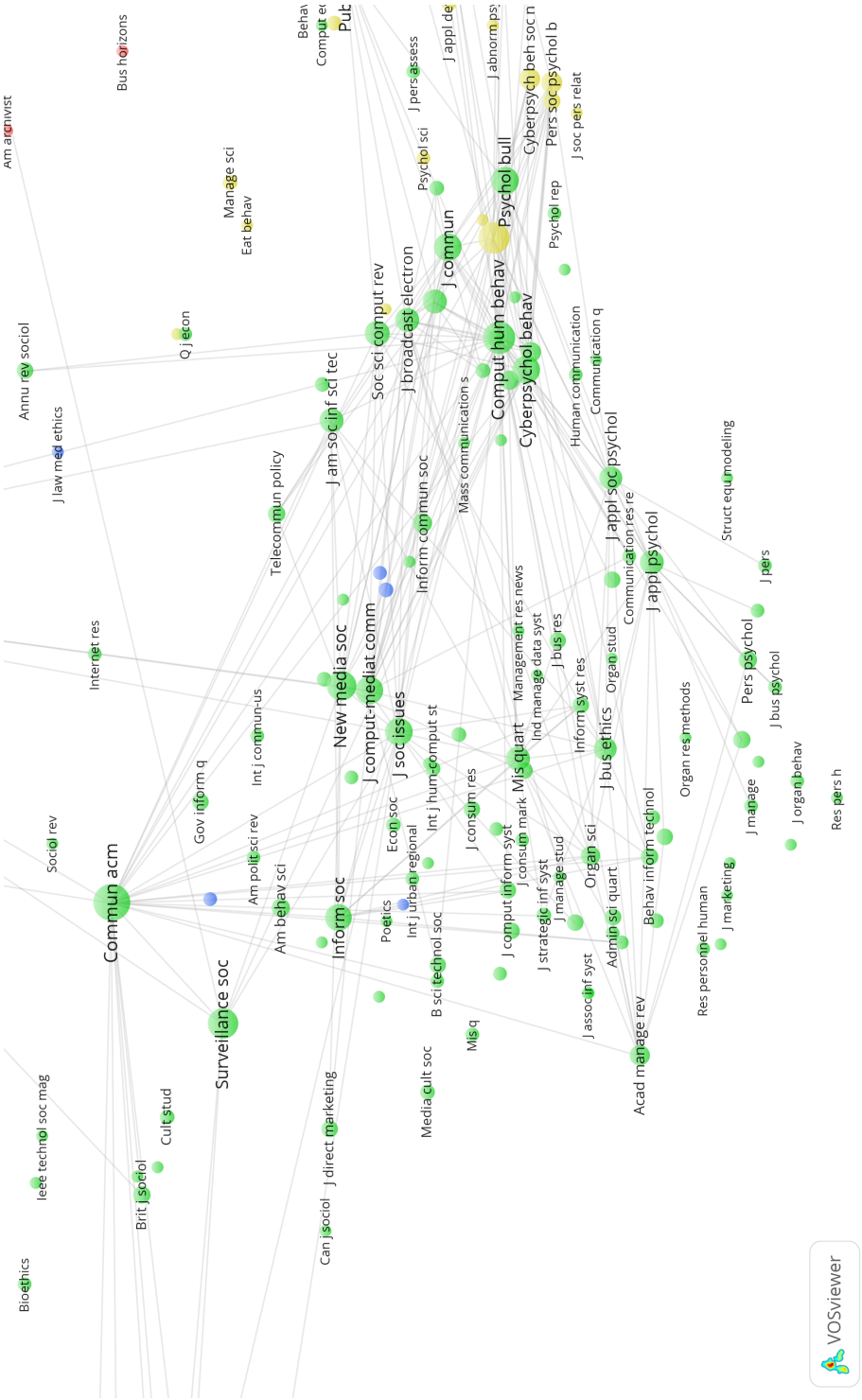
I den högra delen av kartan ovan hittar vi två kluster som framför allt innehåller den medicinskt orienterade forskningen (tillsammans med mer kliniskt orienterad psykologi och psykiatri) som återstår trots försöken att avgränsa sökningen; och som i hög grad rör t.ex. epidemiologisk forskning och forskning kring sjukdoms- och riskbeteenden (från diabetes till könssjukdomar och beroende-orienterad forskning); men också medicinsk- och beteendevetenskaplig forskning som faller inom ramen för vad som är relevant för den här studien. Till vänster på kartan hittar vi ett kluster med juridisk forskning. I den övre delen av kartans mitt finner vi datavetenskaplig

forskning, som i hög utsträckning framför allt handlar om utveckling av system och nätverk, och metoder för signal- och mönsteranalys för övervakning snarare än effekter av övervakningen på individer och frågor om integritet och dylikt (se nedan).



Figur 5. In-zoomning i karta med co-citerade tidskrifter: datavetenskapligt kluster.

Det kluster som kanske är mest intressant utifrån temat för den här studien finner vi i nedre delen av kartans mitt (se nedan). Där samlas forskning representerad av tidskrifter inom informatik, psykologi, management- & marketingforskning, sociologi och annan samhällsvetenskap, samt biblioteks- och informationsvetenskap och medie- och kommunikationsvetenskap.

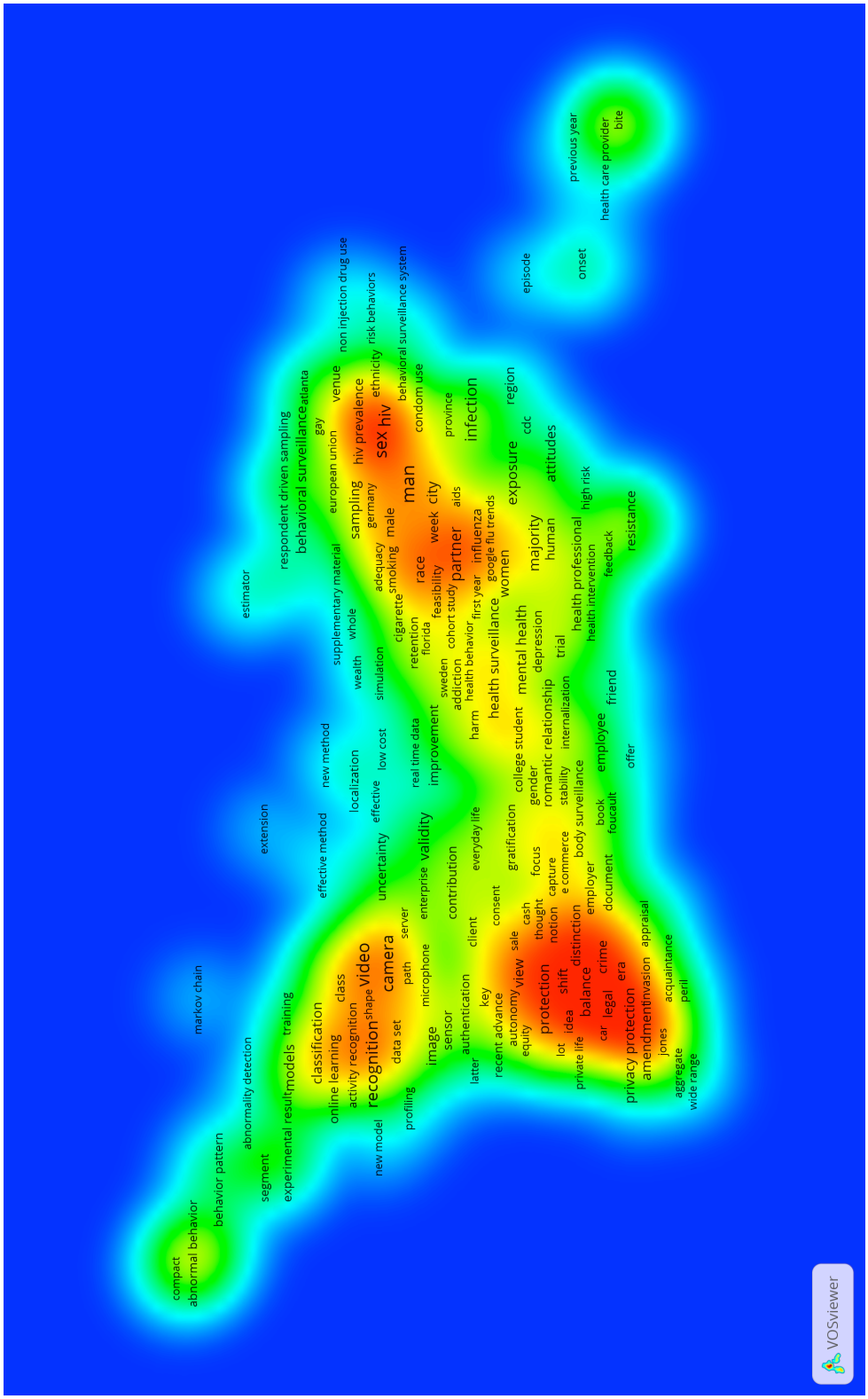


Figur 6. In-zoomning i karta med co-citerade tidskrifter: samhällsvetenskapligt kluster.

Vi kan alltså se en ganska strikt uppdelning av forskning om integritet och övervakning, med tre huvudsakliga fokus: ett tekniskt perspektiv som i hög grad handlar om systemutveckling, ett juridiskt perspektiv med fokus på frågor om lagstiftat skydd av personlig integritet, samt ett mer samhällsvetenskapligt perspektiv som bland annat samlar informatik, psykologi och marketing- och managementforskning. Mellan de olika huvudklustren är det få länkar: man skulle t.ex. kunna tänka sig starkare länkar mellan datavetenskaplig forskning om systemutveckling och den mer användarorienterade informatiken (i hög grad människa-datorinteraktionsforskning) men så är alltså inte fallet. De starkaste länkarna mellan forskningsfält finner vi inom det mer samhällsvetenskapliga klustret, där informatik, psykologi, sociologi, statsvetenskap och marketing- och managementforskning förefaller samverka över disciplinära gränser.

Analys av begrepp
För att gå vidare och identifiera inte bara inom vilka forskningsfält som integritets- och övervakningsfrågor studeras, utan också vad det är man forskar om, gjordes en motsvarande analys som – till skillnad från analysen av forskningsfält – inte bygger på samförekomster av referenser utan istället samförekomster av begrepp. Från artiklarna som identifierats i WoS-sökningen hämtades artiklarnas titlar, abstract och nyckelord som beskriver artiklarnas innehåll. Liksom i den tidigare analysen grupperas de begrepp som förekommer tillsammans i dokumenten.

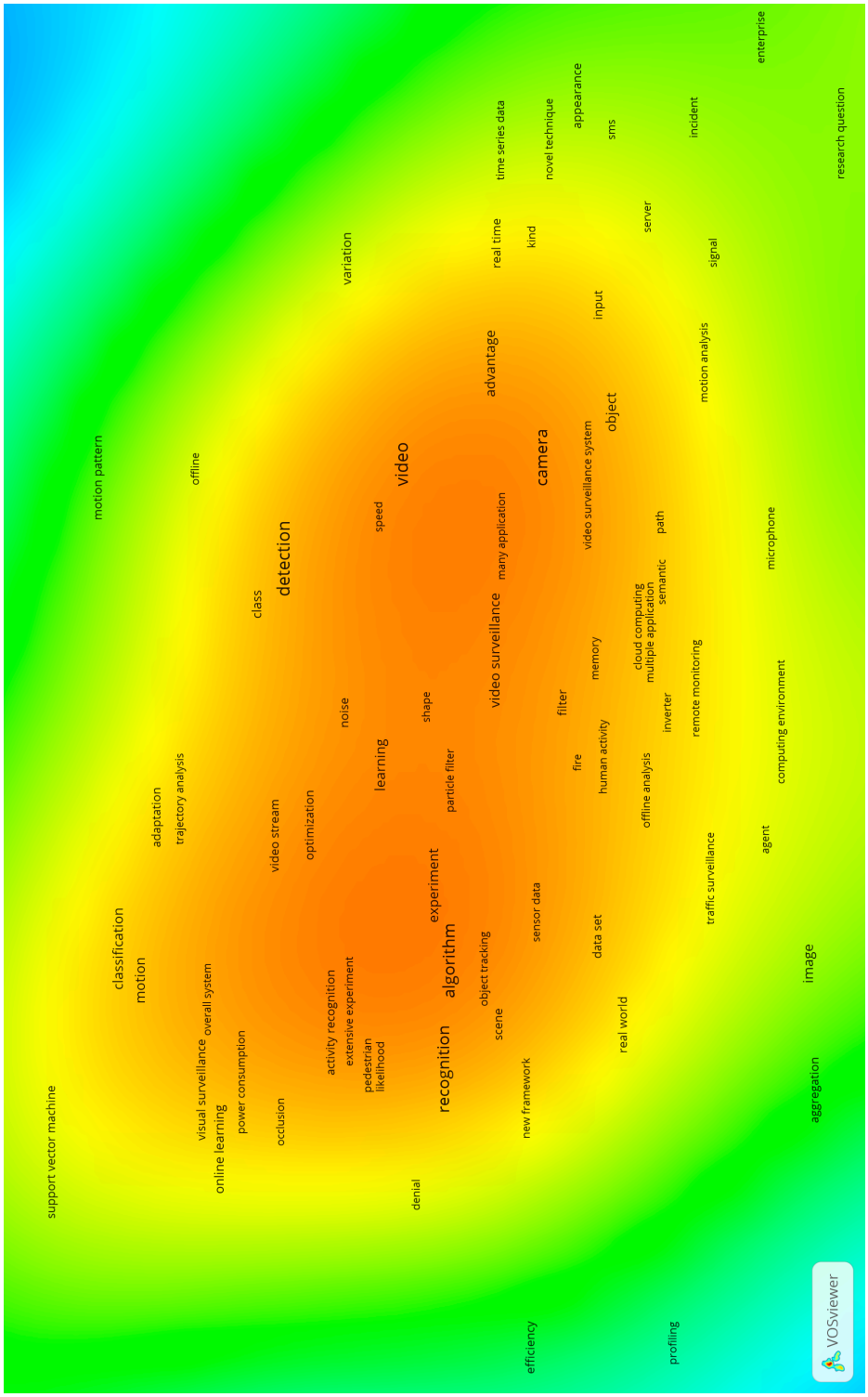
Kartan illustrerar alltså hur de 1465 begrepp som förekommer minst 2 gånger förhåller sig till varandra, de som förekommer ofta tillsammans hamnar närmare varandra på kartan, medan begrepp med lägre grad av samförekomst hamnar längre ifrån. Kartan redovisar också var man hittar större mängder begrepp med starkare samband genom att markera dessa områden med rött, medan områden med färre begrepp och med svagare samband går längre och längre mot grönt och till slut blått.



Figur 7. Samförekomst av begrepp i titlar, abstract samt nyckelord.

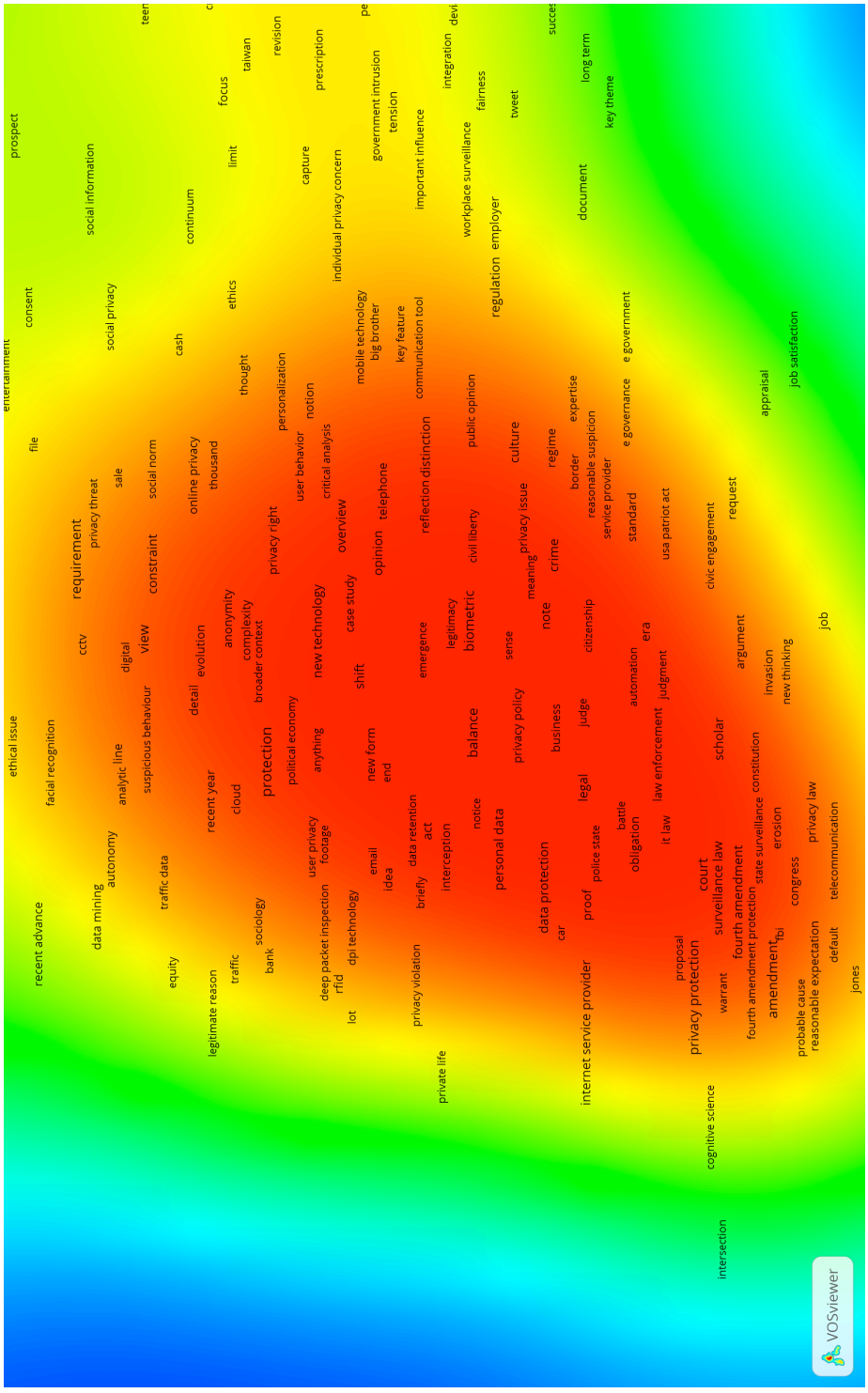
Vi kan se tre huvudsakliga kluster av begrepp på kartan (Figur 7). Till höger finner vi begrepp relaterade till den medicinska forskningen, där övervakning framför allt ska ses som en aspekt av vårdverksamhet för att övervaka eller förhindra spridande av epidemier och för att följa hälsoutveckling, snarare än som en form av kontroll av människor.

I den övre delen av kartans vänstra sida hittar vi ett kluster som motsvarar den teknikvetenskapliga forskningen vi kunde identifiera i vår analys av forskningsfält (Figur 8). Utifrån begreppen i klustret kan vi se att forskningen till stor del handlar om utveckling av system och tekniker för övervakning och igenkänning av mönster i data.



Figur 8. In-zoomning i karta med samförekommande begrepp: datavetenskapligt kluster.

I den nedre delen av kartans vänstra sida hittar vi ett kluster som verkar samla ihop de juridiska och de samhällsvetenskapliga/beteendevetenskapliga forskningsfälten från kartan över forskningsfält. Begreppen knyter an till juridiska, politiska och sociala frågor som skydd av personlig integritet, lagstiftning och förhållande till grundlagar, legitimitet, samt beteenden och sociala normer (Figur 9).



Figur 9. In-zoomning i karta med samförekommande begrepp: samhällsvetenskapligt och juridiskt kluster.

Liksom i kartan över forskningsfälten finner vi få länkar mellan de sociala/samhällsvetenskapliga aspekterna och de mer tekniskt eller medicinska aspekterna, samtidigt som vi kan se att den samhällsvetenskapliga och den juridiska forskningen här begreppsmässigt samlas inom samma kluster. Detta ska dock kanske mer ses som ett tecken på att dessa forskningsfält i hög grad använder samma – och en relativt allmän – terminologi, än att de två forskningsperspektiven aktivt kommunicerar med varandra.

Systematisk litteraturöversikt

Litteratursökningen har uteslutande fokuserat peer-reviewgranskade vetenskapliga artiklar publicerade på engelska under perioden 2005-2015. Peer-review innebär att artiklarna granskas av externa sakkunniga forskare som säkerställer att artiklarna och studierna uppfyller alla krav på vetenskaplig kvalitet. Vi har använt oss av en s.k. booelsk sökning (AND/OR/NOT). De olika databaserna har lite olika funktioner varför sökningar kommer att presenteras separat. Gränssnittet möjliggör sökningar inom antingen/och/eller abstract (AB) och ämnesområde (SU). Genom att göra sökningen i keywords ges möjligheten att fånga upp de texter där författarna själva har specificerat ett antal nyckelord för sin text. Sökningar i denna typ av ämnesord lämpar sig särskilt väl inom områden där det finns en väl etablerad terminologi och samsyn kring innebörden i olika begrepp. Alternativt kan en sökning genomföras i abstract. Detta öppnar upp för möjligheten att söka av ett lite bredare fält där det kanske används lite olika begrepp för att beskriva ungefär samma sak. Samtidigt genererar en bredare sökning ett större material som kommer att behöva avgränsas i nästa steg.

SCOPUS
Sökord och deras inbördes relation relaterar till diskussionerna avseende uppdraget, som beskrevs inledningsvis. Litteratursökningen har uteslutande fokuserat peer-reviewgranskade vetenskapliga artiklar publicerade på engelska under perioden 2005-2015. Genom att använda följande nyckelord: surveillance, internet, online, digital, behaviour, attitudes och privacy genererades följande söksträng:

TITLE-ABS-KEY (((**"Surveillance"**) AND (**"online"** OR **"digital"** OR **"Internet"**) AND (**behaviour** OR **"attitudes"** OR **"privacy"**))) AND DOCTYPE (**ar** OR **re**) AND PUBYEAR > **2004** AND (LIMIT-TO (SUBJAREA , **"SOCI"**) OR LIMIT-TO (SUBJAREA , **"COMP"**) OR LIMIT-TO (SUBJAREA , **"ENGI"**) OR LIMIT-TO (SUBJAREA , **"PSYC"**))

Sökningen genererade 342 artiklar som fördelar sig på följande sätt utifrån publiceringsår:

År	**Antal**
2015	31
2014	55
2013	54
2012	41
2011	45
2010	34
2009	20
2008	23
2007	16
2006	10
2005	13

Sökningen fördelar sig på följande sätt utifrån publikationsland (vilket inte säger något om var forskningen är utförd, eftersom forskare publicerar sig i internationella tidsskrifter):

Publiceringsländer	**Antal**
USA	139
Storbritannien	43
Australien	21
Kina	21
Kanada	19
Italien	11
Sydkorea	10
Nederländerna	9
Taiwan	9
Tyskland	9

Web of Science (core collection)
I denna databas genomfördes sökningen i ”Topic”, vilket inkluderar sökningar i Titlar, Ämnesord och Abstracts. Genom att använda följande nyckelord: surveillance, internet, online, digital, behaviour, attitudes och privacy genererades följande söksträng:

TOPIC: ((("Surveillance") AND (“online" OR "digital" OR "Internet") AND (behaviour OR ”attitudes” OR ”privacy”)))

Refined by: DOCUMENT TYPES: (ARTICLE OR REVIEW)

Vid en första genomgång av sökresultat visar det sig att många av artiklarna har ett fokus på rent medicinska frågeställningar. T ex:

Grigorescu, V. I., D'Angelo, D. V., Harrison, L. L., Taraporewalla, A. J., Shulman, H., & Smith, R. A. (2014). Implementation Science and the Pregnancy Risk Assessment Monitoring System. *Journal of Women's Health*, *23*(12), 989-994.

I syfte att utesluta denna typ av medicinska artiklar använder vi oss av funktionen ”Web of science categories” vilket möjliggör att sortera ut ett antal områden vilka bedöms irrelevanta för frågeställningen. Därmed erhålls en hanterbar mängd artiklar med relevans för uppdraget. Vi bedömer att följande kategorier av journals kan sorteras bort från sökningen:

AND [excluding] **WEB OF SCIENCE CATEGORIES:** (PERIPHERAL VASCULAR DISEASE OR INFECTIOUS DISEASES OR OPTICS OR OBSTETRICS GYNECOLOGY OR TROPICAL MEDICINE OR NUTRITION DIETETICS OR RESPIRATORY SYSTEM OR PARASITOLOGY OR FOOD SCIENCE TECHNOLOGY OR VETERINARY SCIENCES OR UROLOGY NEPHROLOGY OR MEDICINE GENERAL INTERNAL OR SURGERY OR ENDOCRINOLOGY METABOLISM OR CLINICAL NEUROLOGY OR MEDICINE RESEARCH EXPERIMENTAL OR IMMUNOLOGY OR GENETICS HEREDITY OR

DERMATOLOGY OR TOXICOLOGY OR GASTROENTEROLOGY HEPATOLOGY OR PEDIATRICS OR RADIOLOGY NUCLEAR MEDICINE MEDICAL IMAGING OR FISHERIES OR ONCOLOGY OR ZOOLOGY OR PHARMACOLOGY PHARMACY OR CHEMISTRY ANALYTICAL)
Timespan: 2005-2015. **Indexes:** SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.

Resultatet efter automatiserad exkludering blev **330** artiklar, som fördelar sig enligt följande (av databasen angivna områden):

Områden	**Antal**
COMPUTER SCIENCE	63
PSYCHOLOGY	47
PUBLIC ENVIRONMENTAL OCCUPATIONAL HEALTH	43
GOVERNMENT LAW	37
INFORMATION SCIENCE LIBRARY SCIENCE	31
ENGINEERING	30
COMMUNICATION	23
SOCIAL SCIENCES OTHER TOPICS	22
HEALTH CARE SCIENCES SERVICES	22
SCIENCE TECHNOLOGY OTHER TOPICS	18

Publiceringsländer	**Antal**
USA	174
ENGLAND	40
AUSTRALIA	27
CANADA	17
ITALY	16
PEOPLES R CHINA	12
NEW ZEALAND	8
TAIWAN	7
SOUTH KOREA	7
NETHERLANDS	7

År	**Antal**
2015	72
2014	43
2013	42
2012	41
2011	39
2010	30
2008	17
2009	16
2007	13
2006	11

Extrahering och värderingen av materialet

De sammanlagt 672 artiklar, som sökts ut enligt tidigare formulerade kriterier och databaser, importerades sedan och sorteras i referenshanteringssystemet Mendeley. Här genomförs följande sortering.

En första sållning handlar om att ta bort dubletter. Efter utsortering av dubbletter (147 st) fanns 525 artiklar kvar. Därefter sorteras artiklar bort som inte är publicerade på engelska (6 st) varefter det fanns 519 artiklar kvar. På basis av att titlarna inte bedömdes som ämnesrelevanta sorterades sedan 70 artiklar bort, vilket innebar att det efter en första sållning fanns 449 artiklar kvar. Samtliga 449 abstracts skrevs sedan ut och genomgick närläsning. En ny utsortering genomförs enligt följande kategorier:

Y (icke ämnesrelevant) = 260 artiklar sorterades ut.
X (icke en peer-reviewgranskad vetenskaplig artikel) = 17 artiklar sorterades ut.

Kvar blev 172 artiklar kvar för analys. Dessa artiklar lästes i fulltext och kategoriserades av oss utifrån forskningsfokus och studieobjekt. Följande områden identifierades (antalet artiklar anges inom parantes).

Teknik (27)
Lagstiftning (25)
Stat (23)
Generella teoretiska resonemang (21)
Arbete (12)
Kunskap och beteende bland unga (17)
Hälsa (14)
Handel (12)
Privata relationer (9)
Mänskliga rättigheter i det digitala (4)
Sousveillance (3)
Övrigt (5)

Nedan följer en genomgång av respektive fält.

Teknik

27 artiklar

På generellt plan är de artiklar som beskriver den tekniska sidan av övervakning på Internet övervägande utvecklings- och lösningsorienterade. D.v.s. de handlar om hur vi med teknikens hjälp kan utveckla Internet i riktning mot bättre användarvänlighet och integritetsskydd. Begrepp som syftar till att beskriva hur skydd för integriteten kan ”byggas in” i tekniken är ”Trusted computing” (Shiguo et al. 2009; Winkler och Renner 2011), ”Privacy aware design” (Wicker 2011) samt ”Privacy by design” (Cavoukian et al. 2012). Undantagsvis förekommer det artiklar (McKee 2011; Mitchelfelder 2009 och Vitaliev 2007), vilka anlägger ett mer kritiskt perspektiv och lyfter fram det hot som tekniken kan medföra för den personliga integriteten och rätten till privatliv. I syfte att öka medvetenheten och för att komma tillrätta med integritetsfrågor på nätet formuleras följande upprop av McKee (2011, s 287):

”We can change the settings on the software and hardware on our computers and mobile devices (e.g, blocking cookies, turning off location services). We can learn about the specific privacy policies of various sites we use and take action to change our privacy settings. We can find out from some corporations what our behavioral profile is, and we can choose to opt-out of targeted, personalized advertising, either on a site-by-site and company basis or, if the do-not-track option becomes available, then more widely across all the sites we visit. We can choose not to use some sites that have more egregious records of privacy violations. And we can learn more about and use more open-source, non-commercial sites and applications, either those online or ones to be downloaded and hosted on local servers.”

I relation till denna utveckling, mot en teknik som i allt större utsträckning utsätter individens integritet för hot, formulerar även Wicker och Schrader (2011, s 330) ett upprop riktat mot alla ingenjörer att motarbeta utvecklingen: ”Engineers and computer scientists thus have a moral obligation to avoid design choices that are unnecessarily privacy invasive.” De principer som borde vägleda arbetet med att utforma de tekniska aspekterna av framtidens Internet formuleras i termer av ”Privacy-Aware Design Principles” och omfattar fem punkter vilka är tänkta att öka såväl transparans avseende vad som samlas in som möjligheten att påverka vilken information som samlas in:

1) Provide full disclosure of data collection
2) Require consent to data collection
3) Minimize collection of personal data
4) Minimize identification of data with individuals
5) Minimize and secure data retention

På liknande sätt diskuterar Winkler och Renner (2011) hur integritet kan skyddas i termer av ”trusted computing”. Mer specifikt behandlar artikeln videoövervakning av offentliga miljöer i syfte att förebygga brott, samt i relation till detta olika tekniker för att spara och behandla potentiellt integritetskänslig information som genereras genom övervakningen. Det är i

detta sammanhang värt att påpeka att gränsen mellan videoövervakning och övervakning i det digitala blir allt otydligare och teknikerna går in i varandra. Artikeln diskuterar ett antal olika förhållningssätt, t.ex. att data som genereras separareras på ett sätt så att personlig information skiljs från information om beteende: ”personal and behavioral data should be separated directly on the camera. While system operators only get access to behavioral data, a separate stream containing personal data is made available to law enforcement authorities.” alterntativt att bildinformation som kan röja identiteten på en individ automatiskt tas bort genom en s k ”Respectful camera” som detects and blanks people's faces in captured images”. Här beskrivs även ett kryptograferingsverktyg ”PICO” vilket skulle kunna användas för att kryptera integritetskänslig information och där avkryptering av insamlat material endast kunde ske efter det att ett brott begåtts (Winkler och Renner 2011, s 17). Även Babaguchi och Nakashima (2015) behandlar frågan om hur potentiellt integritetskänslig information som samlas in genom videoövervakning kan hanteras. I deras artikel behandlas ett antal konkreta projekt som alla (PriSurv, Digital Diorama (DD), and Mobile Privacy Protection (MPP)) som alla syftar till att stärka individers rätt till privatliv. Ett annat begrepp som förkommer i detta sammanhang är ”Privacy by design” (PbD) där frågor om integritet ”is embedded as a core functionality in the biometric system” Cavoukian et al. (2012). Författarna argumenterar för att frågor om integritet bör utgöra utgångspunkten i arbetet med utvecklingen av ny teknik och nya affärsmodeller, istället för att behandlas i slutskedet eller inte alls.

PbD återkommer även i Shilton (2012) som först och främst behandlar frågan om integritetsfrågor relaterat till användargenerad data. Artikeln beskriver utvecklingen mot att individer genom appar och wearables mäter och kommunicerar t ex motions-, mat- och sömnvanor i sociala nätverk. PbD kan i detta sammanhang innebära att i utvecklingsfasen av denna typ av produkter och tjänster tydligare fokusera hur potentiellt integritetskänslig information kan och bör hanteras. T ex att tydliggöra vilken information som samlas in, men även att underlätta för användaren att själv kunna ställa in hur information samlas, men även hur den kommuniceras.

Shiguo et al. (2009) beskriver den senaste teknikutvecklingen inom området multimedia, vilket inbegriper användarinformation som sparas i samband med vissa tv-tjänster online. Vidare diskuteras olika möjligheter att skydda och hantera känslig information genom t ex olika former av krypteringssystem.

Utifrån ett historiskt perspektiv beskriver Estee (2015) framväxten av olika tekniker för att spåra användares beteende på Internet, från 1990-talet och fram till idag. Med ett särskilt fokus på webbkakor ”cookies” (vilka är textbaserade datafiler med information om användaren som sparas på webbplatsbesökarens dator), hur dessa vuxit fram i olika former samt vilka tekniker som formerats i relation till detta för att skydda användarens integritet. I artikeln lyfts behovet fram av att informera och upplysa ungdomar och studenter om tekniken. I det avslutande kapitlet ”Taking back our digital identities” kan man läsa: ”The implications concern how everyone can continue to interact in online spaces in safe ways and understand how our invisible digital identities are constructed through surfing habits. Those implications include responsibilities to act and teach students about how to protect their identities online. It is up to all of us, as teachers and researchers,

to talk about invisible digital identities with each other and our students." (Estee 2015, s 130).

Andrejevic, M., & Burdon, M. (2015). Defining the Sensor Society. *TELEVISION & NEW MEDIA*, *16*(1, SI), 19–36. http://doi.org/10.1177/1527476414541552

Asiaghi, A. (2009). Materialized surveillance. *Mechanical Engineering*, *131*(3). Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-67650751638&partnerID=tZOtx3y1

BABAGUCHI, N., & NAKASHIMA, Y. (2015). Protection and Utilization of Privacy Information via Sensing. *IEICE Transactions on Information and Systems*, *E98.D*(1), 2–9. http://doi.org/10.1587/transinf.2014MUI0001

Beck, E. N. (2015). The Invisible Digital Identity: Assemblages in Digital Networks. *Computers and Composition*, *35*, 125–140. http://doi.org/10.1016/j.compcom.2015.01.005

Cavoukian, A., Chibba, M., & Stoianov, A. (2012). Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment. *REVIEW OF POLICY RESEARCH*, *29*(1), 37–61. http://doi.org/10.1111/j.1541-1338.2011.00537.x

Chang, R.-I., Wang, T.-C., Wang, C.-H., Liu, J.-C., & Ho, J.-M. (2012). Effective distributed service architecture for ubiquitous video surveillance. *INFORMATION SYSTEMS FRONTIERS*, *14*(3), 499–515. http://doi.org/10.1007/s10796-010-9255-z

Conti, M., Zhang, L., Roy, S., Di Pietro, R., Jajodia, S., & Mancini, L. V. (2009). Privacy-preserving robust data aggregation in wireless sensor networks. *Security and Communication Networks*, *2*(2), 195–213. http://doi.org/10.1002/sec.95

Doyle, T., & Veranas, J. (2014). Public anonymity and the connected world. *ETHICS AND INFORMATION TECHNOLOGY*, *16*(3), 207–218. http://doi.org/10.1007/s10676-014-9346-5

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–15. http://doi.org/10.1007/s11948-014-9551-y

Foresti, G. L., Micheloni, C., Piciarelli, C., & Snidaro, L. (2009). Visual sensor technology for advanced surveillance systems: historical view, technological aspects and research activities in Italy. *Sensors (Basel, Switzerland)*, *9*(4), 2252–70. http://doi.org/10.3390/s90402252

Fuchs, C. (2013). SOCIETAL AND IDEOLOGICAL IMPACTS OF DEEP PACKET INSPECTION INTERNET SURVEILLANCE. *INFORMATION COMMUNICATION & SOCIETY*, *16*(8), 1328–1359. http://doi.org/10.1080/1369118X.2013.770544

H. Dutton, W. (2014). Putting things to work: social and policy challenges for the Internet of things. *Info*, *16*(3), 1–21. http://doi.org/10.1108/info-09-2013-0047

Hossain, M. A. (2014). Framework for a Cloud-Based Multimedia Surveillance System. *International Journal of Distributed Sensor Networks*, *2014*, 1–11. http://doi.org/10.1155/2014/135257

Kim, H., Giacomin, J., & Macredie, R. (2014). A Qualitative Study of Stakeholders' Perspectives on the Social Network Service Environment. *International Journal of Human-Computer Interaction*, *30*(12), 965–976. http://doi.org/10.1080/10447318.2014.925383

Leo, M., D'Orazio, T., Caroppo, A., Martiriggiano, T., & Spagnolo, P. (2005). Automatic monitoring of forbidden areas to prevent illegal accesses. In P. Singh, S and Singh, M and Apte, C and Perner (Ed.), *PATTERN RECOGNITION AND IMAGE ANALYSIS, PT 2, PROCEEDINGS* (Vol. 3687, pp. 635–643).

McKee, H. A. (2011). Policy Matters Now and in the Future: Net Neutrality, Corporate Data Mining, and Government Surveillance. *Computers and Composition*, *28*(4), 276–291. http://doi.org/10.1016/j.compcom.2011.09.001

Michelfelder, D. P. (2009). Philosophy, privacy, and pervasive computing. *AI & SOCIETY*, *25*(1), 61–70. http://doi.org/10.1007/s00146-009-0233-2

Moradoff, N. (2010). Biometrics: Proliferation and constraints to emerging and new technologies. *SECURITY JOURNAL*, *23*(4), 276–298. http://doi.org/10.1057/sj.2008.21

Mordini, E., & Rebera, A. P. (2012). No Identification Without Representation: Constraints on the Use of Biometric Identification Systems. *REVIEW OF POLICY RESEARCH*, *29*(1), 5–20. http://doi.org/10.1111/j.1541-1338.2011.00535.x

Morris, B. T., & Trivedi, M. M. (2011). Trajectory learning for activity understanding: unsupervised, multilevel, and long-term adaptive approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *33*(11), 2287–301. http://doi.org/10.1109/TPAMI.2011.64

Nguyen, H. T. M. (2011). CLOUD COVER: PRIVACY PROTECTIONS AND THE STORED COMMUNICATIONS ACT IN THE AGE OF CLOUD COMPUTING. *NOTRE DAME LAW REVIEW*, *85*(6), 2189–2218.

Shiguo, L., Kanellopoulos, D., & Ruffo, G. (2009). Recent advances in multimedia information system security. *Informatica (Ljubljana)*, *33*(1), 3–24. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-64249107623&partnerID=tZOtx3y1

Shilton, K. (2012). Participatory personal data: An emerging research challenge for the information sciences. *JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY*, *63*(10), 1905–1915. http://doi.org/10.1002/asi.22655

Vitaliev, D. (2007). Big brother is watching you [Internet security]. *Communications Engineer*, *5*(5), 20–25. http://doi.org/10.1049/ce:20070502

Weaver, S. D., & Gahegan, M. (2007). Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*, *97*(3), 324–350. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-36849064241&partnerID=tZOtx3y1

Wicker, S. B., & Schrader, D. E. (2011). Privacy-Aware Design Principles for Information Networks. *Proceedings of the IEEE*, *99*(2), 330–350. http://doi.org/10.1109/JPROC.2010.2073670

Winkler, T., & Rinner, B. (2011). Securing Embedded Smart Cameras with Trusted Computing. *EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING*. http://doi.org/10.1155/2011/530354

Lagstiftning

25 artiklar

På ett övergripande plan behandlar i princip samtliga artiklar rättens oförmåga att skydda individens rättigheter till följd av snabba framväxten av digital teknologi. En central fråga, för de artiklar som rör förhållanden i USA, avseende legala av aspekter av den digitala tekniken och hot om att inskränka den personliga integriteten, är ”the Fourth Amendment” (Desai 2014; Hu 2013; Kerr 2010; Solove 2005); som utgör en viktig del av den amerikanska konstitutionen. Den del av Fourth amendment som diskuteras i detta sammanhang rör individens rätt till privatliv. Utgångspunkten i samtliga artiklar är antagandet att den digitala teknikutvecklingen medfört att lagen inte längre på ett fullgott sätt förmår att skydda individens rätt till privatliv.

Kerr (2010) söker att applicera konstitutionen och the Fourth Amendment på en Internet-relaterad kontext och tar sin utgångspunkt i de otydligheter som existerar avseende vilken typ av digital kommunikation (t ex e-post och sms) som skyddas från övervakning av lagen. Ambitionen är att söka skapa ett system som ger ett lika stort skydd i den digitala världen som i den fysiska. Mer specifikt diskuterats distinktionen mellan ”Inside” och ”Outside” i en polisundersökning. Termerna beskriver individens förväntningar på privatliv och polisens rättigheter att observera och samla in information om individers beteende, i relation till vilken fysisk miljö individen befinner sig i. Lagen gör skillnad på rätt till privatliv beroende av huruvida du rör dig i ett offentligt utrymme eller i ditt eget hus. Frågan som diskuteras i artikeln är följaktligen hur denna distinktion ska översättas i en digital kontext.

Även Desai (2014) diskuterar individens rätt till privatliv i relation till polisutredningar men i termer av ”Forward looking” och ”Backward looking” övervakning. Forward looking övervakning beskriver den typ av övervakning som sker med ett speciellt tillstånd av en domare och omfattar t ex GPS-övervakning och telefonavlyssning. För att få till stånd ett sådant krävs misstanke om någon form av kriminell handling. Vidare anger tillståndet vilken typ av information som får samlas in samt i vilket syfte den kan användas. Problemet som diskuteras i artikeln avser backward looking vilket beskrivs på följande sätt: ” With backward-looking surveillance all these protections are gone. Law enforcement or intelligence services need only ask a business for the record of where we went, whom we called, what we read, and more. They then have a near perfect picture of our activities and associations regardless of whether they are criminal. There is thus an asymmetry that makes little sense.” (Desai 2014, s. 582-583). Framförallt beskrivs detta sätt att tämligen enkelt skapa en detaljerad bild över en individs liv vara ett hot mot att organisera och uttrycka sig politiskt.

Ett annat centralt tema i de artiklar som behandlar lagstiftning är rätten till data (Cover 2015; Grodzinsky och Tavani 2005; Konstadinides 2011; Mantalero 2014; Peppet 2014; Roberts 2015). Utgångspunkten är den oklarhet som råder avseende vem som äger information som genereras när man agerar på nätet, samt vem som har rätt till dessa data och i vilket syfte den får användas. Mantelero (2014, s. 644) formulerar problematiken på följande sätt: ”However, the high demand for personal information, the

complexity of the new tools of analysis and the increasing numbers of sources of data collection, have generated an environment in which the 'data barons' (i.e. big companies, government agencies, intermediaries) have a control over digital information which is no longer counterbalanced by the user's self-determination." Den lagstiftning som är tänkt att skydda individens rätt till integritet i sammanhanget bygger på principen "Notice and consent", d.v.s. användaren ska ha rätt till att bli informerad om vilken data som samlas in och även ha möjlighet att ge samtycke eller ej. Problem med Notice and consent i detta sammanhang beskriver Mantelero (2014, s. 652) som: "Since Big Data analytics are designed to extract hidden or unpredictable inferences and correlations from datasets, the description of these purposes is becoming more and more "evanescent". This is a consequence of the "transformative" use of Big Data, which makes it often impossible to explain all the possible uses of data at the time of its initial collection." Med andra ord har den så kallade handeln med data inneburit att den hamnar i nya sammanhang än vad som från början var avsett. Detta i kombination med att data från olika sammanhang sammanförs och analyseras kan mönster om såväl individer som grupper avtäckas. Peppet (2014) adresserar framväxten av "Internet of things" samt potentiella problem med hur data lagras och används i detta sammanhang. Internet of things är en samlingsterm för datorbaserad teknik inbyggd i produkter (ofta bärbara) som registrerar vardagliga aktiviteter såsom motions-, mat- och sömnvanor. I detta sammanhang frågar sig författaren "As the Internet of Things generates ever more massive and nuanced datasets about consumer behavior, how to protect privacy? How to deal with the reality that sensors are particularly vulnerable to security risks? How should the law treat and how much should policy depend upon consumer consent in a context in which true informed choice may be impossible?" (Peppet 2014, s. 85).

Brown, I. (2010). Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, *19*(2), 95–109. http://doi.org/10.1093/ijlit/eaq016

Cheng, F.-C., & Lai, W.-H. (2010). An overview of VoIP and P2P copyright and lawful-interception issues in the United States and Taiwan. *Digital Investigation*, *7*(1-2), 81–89. http://doi.org/10.1016/j.diin.2010.08.001

Coudert, F. (2009). Towards a new generation of CCTV networks: Erosion of data protection safeguards? *Computer Law & Security Review*, *25*(2), 145–154. http://doi.org/10.1016/j.clsr.2009.02.003

Cover, A. Y. (2015). Corporate Avatars and the Erosion of the Populist Fourth Amendment. *IOWA LAW REVIEW*, *100*(4), 1441–1502.

Desai, D. R. (2014). CONSTITUTIONAL LIMITS ON SURVEILLANCE: ASSOCIATIONAL FREEDOM IN THE AGE OF DATA HOARDING. *NOTRE DAME LAW REVIEW*, *90*(2), 579–632.

Fairfield, J. A. T., & Luna, E. (2014). DIGITAL INNOCENCE. *CORNELL LAW REVIEW*, *99*(5), 981–1076.

Garlinger, P. P. (2009). PRIVACY, FREE SPEECH, AND THE PATRIOT ACT: FIRST AND FOURTH AMENDMENT LIMITS ON NATIONAL SECURITY LETTERS. *NEW YORK UNIVERSITY LAW REVIEW*, *84*(4), 1105–1147.

Grodzinsky, F. S., & Tavani, H. T. (2005). P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property. *Ethics and Information Technology*, *7*(4), 243–250. http://doi.org/10.1007/s10676-006-0012-4

Hayes, A. S. (2014). The USPS as an OSP: A Remedy for Users' Online Privacy Concerns. *Communication Law and Policy*, *19*(4), 465–507. http://doi.org/10.1080/10811680.2014.955770

Hu, M. (2013). Biometric ID Cybersurveillance. *INDIANA LAW JOURNAL*, *88*(4), 1475–1558.

Kerr, O. S. (2010). APPLYING THE FOURTH AMENDMENT TO THE INTERNET: A GENERAL APPROACH. *STANFORD LAW REVIEW*, *62*(4), 1005–1049.

Kierkegaard, S. (2005). Privacy in electronic communication. *Computer Law & Security Review*, *21*(3), 226–236. http://doi.org/10.1016/j.clsr.2005.04.008

Konstadinides, T. (2011). Destroying democracy on the ground of defending It? the Data Retention Directive, the surveillance state and our constitutional ecosystem. *European Law Review*, *36*(5), 722–736. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84868150276&partnerID=tZOtx3y1

Mantelero, A. (2014). The future of consumer data protection in the EU Re-thinking the ``notice and consent{''} paradigm in the new era of predictive analytics. *COMPUTER LAW & SECURITY REVIEW*, *30*(6), 643–660. http://doi.org/10.1016/j.clsr.2014.09.004

Nguyen, H. T. M. (2011). CLOUD COVER: PRIVACY PROTECTIONS AND THE STORED COMMUNICATIONS ACT IN THE AGE OF CLOUD COMPUTING. *NOTRE DAME LAW REVIEW*, *85*(6), 2189–2218.

Ojanen, T. (2014). Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Right. *EUROPEAN CONSTITUTIONAL LAW REVIEW*, *10*(3), 528–541. http://doi.org/10.1017/S1574019614001345

Peppet, S. R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *TEXAS LAW REVIEW*, *93*(1), 85–178.

Riedy, M. K., & Wen, J. H. (2010). Electronic surveillance of Internet access in the American workplace: implications for management. *Information & Communications Technology Law*, *19*(1), 87–99. http://doi.org/10.1080/13600831003726374

Roberts, A. (2015). Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications. *MODERN LAW REVIEW*, *78*(3), 535–548. http://doi.org/10.1111/1468-2230.12127

Robison, W. J. (2010). Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act. *GEORGETOWN LAW JOURNAL*, *98*(4), 1195–1239.

Saxby, S. (2014). The 2013 CLSR-LSPI seminar on electronic identity: The global challenge - Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11-15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand. *COMPUTER LAW & SECURITY REVIEW*, *30*(2), 112–125. http://doi.org/10.1016/j.clsr.2014.01.007

Schlabach, G. R. (2015). PRIVACY IN THE CLOUD: THE MOSAIC THEORY AND THE STORED COMMUNICATIONS ACT. *STANFORD LAW REVIEW*, *67*(3), 677–721.

Solove, D. J. (2005). Fourth Amendment codification and Professor Kerr's misguided call for judicial deference. *FORDHAM LAW REVIEW*, *74*(2), 747–777.

Stalla-Bourdillon, S. (2013). Online monitoring, filtering, blocking ….What is the difference? Where to draw the line? *Computer Law & Security Review*, *29*(6), 702–712. http://doi.org/10.1016/j.clsr.2013.09.006

Stalla-Bourdillon, S., Papadaki, E., & Chown, T. (2014). From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy … The case of deep packet inspection technologies. *Computer Law & Security Review*, *30*(6), 670–686. http://doi.org/10.1016/j.clsr.2014.09.006

Stat

23 artiklar

Gemensamt för de artiklar som behandlar frågan om relationen mellan stat och medborgare i en digital kontext är hur och i vilka sammanhang det kan betraktas som legitimt för staten att aktivt samla in information avseende individers kommunikation på Internet, samt vilka konsekvenserna kan tänkas bli i termer av bristande tillit och politiskt engagemang när övervakningen upplevs som obefogad eller alltför långtgående. De svar som forskningen ger inom detta område är dock inte helt samstämmiga utan kräver att man tar hänsyn till enskilda länders specifika förhållanden samt interaktionen mellan upplevd nytta med övervakning och ålder, utbildning, yrke och politiska åsikter.

I fallet Kina där den totalitära enpartistaten i sig, ur ett rent demokratiperspektiv, är illegitim diskuteras frågor om övervakning som rena maktmedel för att stärka statens ställning visavi medborgarna (Jiang och Okamoto 2014; Wang och Hong 2010). I en av artiklarna (Jiang och Okamoto 2014) beskrivs att av Kinas sammanlagt 1,3 miljarder invånare är 42 % internetanvändare. Hos dessa 591 miljoner internetanvändare är web-sökningar genom olika sökmotorer en av de vanligaste aktiviteterna. Jiang och Okamotos (2014) artikel fokuserar den statliga sökmotorn Jike, vilken beskrivs av författarna som ett försök av Kinas kommunistiska parti (KKP) ”to control information, enhance legitimacy and achieve cyber power through both technological regulation and creation” (s 100). Enligt artikelförfattarna uppnås ”cyber power” genom att (1) förstärka nationell identitet och solidaritet genom sökmotorns nationalistiska gränssnitt (2) genom vilka sökresultat som förmedlas, samt (3) genom dess potential att spionera på hur användarna beter sig på nätet. De första två punkterna beskrivs tämligen ingående i artikeln emedan frågan om hur information om sökmotorns användare lagras och används diskuteras på en mer hypotetisk nivå. Detta då det inte, enligt författarna, är känt vilken typ av information som lagras samt hur denna används.

Wang och Hong (2010) fokuserar den Kinesiska bloggsfären utifrån frågor om huruvida detta forum för kommunikation möjligtvis kan bidra till en ökad öppenhet i landet. Författarna utmanar bilden av bloggar och bloggare som samhällsomvandlare och menar att den kinesiska staten framgångsrikt begränsat vad som kan uttryckas i detta medium. ”The expansion of China’s use of cyberspace is matched by the government’s efforts to control, censor, and repress it with strict legislation, jailing cyber-dissidents, spying on discussions, filtering content, and barring access to websites with the help from the Western companies who provide the mechanism through the open market. Although China’s Bloggers are empowered by this new communication vehicle, which allows them to express themselves freely and deliberately, China’s blogosphere is not leading to the overthrow of the dictatorship (s. 76).

Artiklarna som diskuterar förhållandena i Kina är starkt kritiska till landets regim och ett underliggande antagande som är genomgående är att

övervakning av medborgare på Internet i huvudsak syftar till att stärka KKPs makt och inte till att skydda medborgarna mot yttre hot.

Frågan om yttre hot samt statens möjlighet att förebygga dessa genom övervakning på Internet är ett tydligt tema också för den forskning och de artiklar som behandlar medborgare-stat i USA. Utgångspunkten i Redick et al. (2015) är den debatt som uppstod avseende den massövervakning som utförs av National Security Agency (NSA), vilken i stora delar skedde utan medborgarnas vetskap. Ett underliggande antagande i denna artikel är att övervakningen i sig är legitim och syftar till att förbättra statens funktionsförmåga: ”public sector organizations are increasingly using data to improve their performance, provide greater citizen engagement, and cultivate levels of collaboration and transparency.” (s. 129). Utgångspunkten är med andra ord att långtgående övervakning av medborgarna var (och är) legitim, samt att utmaningen snarare handlar om att förbättra hur övervakningsprogrammen kommuniceras: ”These findings indicate that government needs to be more efficacious in communicating about surveillance programs more transparently to garner greater citizens' approval for its surveillance programs” (s. 138).

Följaktligen kommer attityden till övervakning att påverkas av i vilken mån den upplevs som legitim. Legitimiteten i sig är sin tur relaterat till upplevd hotbild samt statens förmåga att genom övervakning av medborgare förebygga och bemöta dessa hot. En slutsats som formuleras av Dinev et al. (2008, s. 214) ”The perceived need for government surveillance was negatively related to privacy concerns and positively related to willingness to disclose personal information.” Bilden av att det finns en tämligen långtgående acceptans för statlig övervakning i USA stärks även i Dinev et al. (2006), som genomfört en komparativ studie över attityder till övervakning mellan Italien och USA. Författarna konkluderar att ”Italians exhibit lower Internet privacy concerns than individuals in the U.S., lower perceived need for government surveillance, and higher concerns about government intrusion. (s 1)”. Italienarnas motvilja till statlig övervakning förklaras i artikeln dels genom en lägre upplevd risk men även med en lägre grad av tillit till staten.

I två studier avseende medborgarnas syn på statlig övervakning på Internet i Balkanländerna (Budak et al. 2013; Budak et al., 2015) visar på vikten av att ta hänsyn till olika demografiska förhållanden för att kunna förstå och förklara attityder till övervakning. I deras analys kan medborgarna delas in i tre grupper: “(1) pro-surveillance oriented citizens, (2) citizens concerned about being surveilled and (3) citizens opting for better data protection” (s 17). Dessa grupper skiljer sig åt beroende av ålder, utbildning och yrke. Exempelvis visar den statistiska analysen att medborgare med en lägre utbildningsnivå tenderade att vara mer “pro-surveillance” än de med högre utbildning. På samma sätt visar det sig sig att de som står utanför arbetsmarknaden tenderade att vara för övervakning i större utsträckning än de som lönearbetade. Vad gäller ålder visar det sig att yngre medborgare var “pro-surveillance” i större utsträckning än äldre. Samtidigt uttrycker även gruppen yngre viss oro för risken att vara övervakad.

Cohrs et al. (2005) fördjupar förståelsen för hur upplevelsen av yttre hot påverkar attityder till övervakning. Här argumenteras delvis mot Redik et al.

(2015) och Cohrs et al. (2005) menar att enbart upplevelse av hot inte nödvändigtvis påverkar attityder till övervakning.

En annan central fråga som avhandlas i de artiklar som diskuterar relationen mellan stat och medborgare är huruvida upplevelsen av att vara övervakad på Internet påverkar det politiska engagemanget. Här är resultaten tämligen motstridiga. Best och Krueger (2008) argumenterar för att rädslan för övervakning är ett reellt hot mot demokratin i det att det påverkar det politiska engagemanget. "The findings suggest that the prospects of govemment surveillance may, in fact, be a consideration in U.S. citizens' decisions to participate politically. Concerned that the government may monitor such nonviolent activities, citizens may choose to avoid them, particularly compared to more anonymous political activities such as voting. Moreover, those who disapprove of the president are more likely to perceive govemment monitoring and are more likely to perceive that the govemment uses comparatively invasive techniques when monitoring. Therefore any 'chilling effect' would not be distributed randomly across the political spectrum, which potentially damages the often-cited ideal of equal consideration." (Best och Krueger 2008, s 205).

Det finns dock studier som visar upp delvis motsatta resultat. Krueger (2005) visar att det största politiska engagemanget online uppvisar de grupper som upplever störst problem med hot om statlig övervakning. "Those most out of step with dominant opinion, who also feel that the government monitors citizens' Internet activity, participate in politics online at the highest rates." Krueger (2005, s 448).

Ett upplevt hot om övervakning och bristande tillit till statens förmåga att hantera känslig information om medborgarna är även en central fråga inom området E-förvaltning (E-government). E-förvaltning är ett samlingsbegrepp för statens arbete att, med hjälp av informations och kommunikationsteknologi, förenkla och förbättra samhällsservicen till medborgare och företag samt att underlätta för medborgare att få tillgång till information och aktivt delta i beslutsprocesser i den offentliga förvaltningen. Rädslan för hur staten använder personlig och känslig information som genereras av medborgarna på Internet kan påverka tilliten mellan parterna och i förlängningen viljan att använda sig av olika e-tjänster. Detta är budskapet i Keymolen et al. (2012) som inte redovisar någon egen data, utan för diskussioner på ett mer teoretiskt plan, samt går igenom mer konkreta exempel på saker att ta hänsyn till, för att stärka tilliten mellan stat och medborgare, samt i förlängningen öka viljan att ta del av digitala tjänster och dela med sig av känslig information online. Lips (2010) argumenterar för att det finns en betydande acceptans, vad gäller att dela med sig av personlig information till staten, så länge detta leder till bättre samhällstjänster. För att detta utbyte mellan information om medborgarna och samhällstjänster ska fungera smidigt måste transparensen öka avseende vilken information som samlas in samt i vilket syfte den används. Haikola och Jonsson (2007) presenterar en studie över hur debatten fördes i Sveriges riksdag avseende relation mellan individens rätt till integritet och behovet av övervakning vid tiden för Internets framväxt. De argumenterar för att även om röster mot ökad övervakning förkom var de ändå i minoritet i relation till den rådande diskursen som inbegrep en bild om ett ökat behov av insamling av information gällande medborgarna.

Bedi, M. (2014). SOCIAL NETWORKS, GOVERNMENT SURVEILLANCE, AND THE FOURTH AMENDMENT MOSAIC THEORY. *BOSTON UNIVERSITY LAW REVIEW*, *94*(6), 1809–1880.

Best, S. J., & Krueger, B. S. (2008). Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms. *Journal of Information Technology & Politics*, *5*(2), 191–212. http://doi.org/10.1080/19331680802294479

Budak, J., Anic, I.-D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *INNOVATION-THE EUROPEAN JOURNAL OF SOCIAL SCIENCE RESEARCH*, *26*(1-2, SI), 100–118. http://doi.org/10.1080/13511610.2013.723404

Budak, J., Rajh, E., & Anic, I.-D. (2015). Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens. *JOURNAL OF BALKAN AND NEAR EASTERN STUDIES*, *17*(1), 29–48. http://doi.org/10.1080/19448953.2014.990278

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Government surveillance disclosures, bilateral trust and Indonesia-Australia cross-border security cooperation: Social network analysis of Twitter data. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 118–128. http://doi.org/10.1016/j.giq.2015.01.002

Cheng, F. C., & Lai, W. H. (2012). The observation of regulatory approach within internet activities in the United States. *International Journal of Advancements in Computing Technology*, *4*(15), 421–428. http://doi.org/10.4156/ijact.vol4.issue 15.49

Cheng, F.-C., & Lai, W.-H. (2010). An overview of VoIP and P2P copyright and lawful-interception issues in the United States and Taiwan. *Digital Investigation*, *7*(1-2), 81–89. http://doi.org/10.1016/j.diin.2010.08.001

Citron, D. K. (2010). Fulfilling government 2.0's promise with robust privacy protections. *George Washington Law Review*. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-77955341233&partnerID=tZOtx3y1

Cohrs, J. C., Kielmann, S., Maes, J., & Moschner, B. (2005). Effects of Right-Wing Authoritarianism and Threat from Terrorism on Restriction of Civil Liberties. *Analyses of Social Issues and Public Policy*, *5*(1), 263–276. http://doi.org/10.1111/j.1530-2415.2005.00071.x

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *JOURNAL OF GLOBAL INFORMATION MANAGEMENT*, *14*(4), 57–93. http://doi.org/10.4018/jgim.2006100103

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, *17*(3), 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Ebenger, T. (2008). The USA PATRIOT Act: Implications for Private E-Mail. *Journal of Information Technology & Politics*, *4*(4), 47–64. http://doi.org/10.1080/19331680801978759

Haikola, S., & Jonsson, S. (2007). State surveillance on the internet - The Swedish debate and the future role of libraries and LIS. *LIBRI*, *57*(4), 209–218. http://doi.org/10.1515/LIBR.2007.209

Irion, K. (2009). Privacy and securityInternational communications surveillance. *Communications of the ACM*, *52*(2), 26. http://doi.org/10.1145/1461928.1461940

Jiang, M., & Okamoto, K. (2014). National Identity, Ideological Apparatus, or Panopticon? A Case Study of the Chinese National Search Engine Jike. *Policy & Internet*, *6*(1), 89–107. http://doi.org/10.1002/1944-2866.POI353

Kang, S., & Gearhart, S. (2010). E-Government and Civic Engagement: How is Citizens' Use of City Web Sites Related with Civic Involvement and Political Behaviors? *JOURNAL OF BROADCASTING & ELECTRONIC MEDIA*, *54*(3), 443–462. http://doi.org/10.1080/08838151.2010.498847

Keymolen, E., Prins, C., & Raab, C. (2012). Trust and ICT: New challenges for public administration. *Innovation and the Public Sector*, *19*, 21–35. http://doi.org/10.3233/978-1-61499-137-3-21

Krueger, B. S. (2005). Government surveillance and political participation on the Internet. *SOCIAL SCIENCE COMPUTER REVIEW*, *23*(4), 439–452. http://doi.org/10.1177/0894439305278871

Lips, M. (2010). Rethinking citizen-government relationships in the age of digital identity: Insights from research. *Information Polity*, *15*(4), 273–289. http://doi.org/10.3233/IP-2010-0216

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 129–141. http://doi.org/10.1016/j.giq.2015.01.003

Ventura, H. E., Miller, J. M., & Deflem, M. (2005). Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power. *Critical Criminology*, *13*(1), 55–70. http://doi.org/10.1007/s10612-004-6167-6

Wang, S. S., & Hong, J. (2010). Discourse behind the Forbidden Realm: Internet surveillance and its implications on China's blogosphere. *Telematics and Informatics*, *27*(1), 67–78. http://doi.org/10.1016/j.tele.2009.03.004

Xu, H., & Dinev, T. (2012). The security-liberty balance: individuals' attitudes towards internet government surveillance. *Electronic Government, an International Journal*, *9*(1), 46. http://doi.org/10.1504/EG.2012.044778

Generella teoretiska resonemang

21 artiklar

De artiklar som samlas under denna rubrik har det gemensamt att de inte först och främst presenterar egen empiri, utan främst för övergripande teoretiska diskussioner avseende framväxten av vad som av många benämns som övervakningssamhället. Då texterna i huvudsak bygger på sammanhängande resonmang över cirka 15 sidor, blir det svårt att på ett enkelt sätt sammanfatta innehållet här. Två återkommande begrepp är emellertid Pantopticon och Big Brother.

Den digitala teknikens stora möjligheter, för centrala aktörer, att följa enskildas beteenden beskrivs även i flera andra artiklar i termer av Pantopticon (Farinosi 2014; Ganascia 2010; Grodzinsky och Tavani 2005; Humphreys 2006; Kandias et al. 2014; Jiang och Okamoto 2014; Russett 2011). Det digitala samhället problematiseras här utifrån det faktum att det möjliggör massiv övervakning av samhällets alla medborgare. Men här beskrivs också hur de digitala strukturera kan användas av var och en och på så sätt stärka individens makt i förhållande till makten.

Ego-Panopticism: beskrivs som en ökad möjlighet för enskilda individer att, genom det digitala mediet, övervaka och sprida information avseende missförhållanden och maktmissbruk i samhället. Med andra ord ett omvänt panopticon, eller som de skriver **"**counter-panopticism". Panopticism syftar i detta fall tillbaka på Jeremy Benthams modell över det ideala fängelset där fången alltid (i vart fall potentiellt) är betraktad av övervakaren. "The individual is now an operative in the surveillance society so political and social elites are at risk of disclosure of aberrant behavior through instantaneous disclosure by any random witness. Accordingly, technology has created an evolution in societal power relationships." (Smith et al. 2011, s).

Big brother: Även Orwells dystopiska bild av det framtida övervakningssamhället som återfinns i romanen 1984 är flitigt refererad (Giroux 2015; Kang et al. 2012; Mordini och Rebera 2012; Stančin och Tomažič 2010; Van Otterlo 2014; Vitaliev 2007). I Zuboff 2015 används termern Big brother för att beskriva baksidorna med den flitiga handeln med och akumulation av potentiellt integritetskänslig personlig information. Då användardata samlas in i olika sammanhang för att sedan säljas vidare blir det följaktligen otydligt vem som har information om mig samt vilka konsekvenser detta kan medföra. Detta bekskrivs även i termer av Surveillance capitalism: "Surveillance capitalism offers a new regime of comprehensive facts and compliance with facts. It is, I have suggested, a *coup* from above – the installation of a new kind of sovereign power." (Zuboff 2015, s 86).

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies*, *13*(1), 5–24. http://doi.org/10.1177/1367877909348536

Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, *6*(2), 119–134. http://doi.org/10.1177/1477370808100541

De Laat, P. B. (2008). Online diaries: Reflections on trust, privacy, and exhibitionism. *Ethics and Information Technology*, *10*(1), 57–69. http://doi.org/10.1007/s10676-008-9155-9

Earl, J. (2012). PRIVATE PROTEST? Public and private engagement online. *INFORMATION COMMUNICATION & SOCIETY*, *15*(4, SI), 591–608. http://doi.org/10.1080/1369118X.2012.665936

Ellis, D., Harper, D., & Tucker, I. (2013). The Dynamics of Impersonal Trust and Distrust in Surveillance Systems. *Sociological Research Online*, *18*(3). http://doi.org/10.5153/sro.3091

Farinosi, M. (2011). Deconstructing bentham's panopticon: The new metaphors of surveillance in the web 2.0 environment. *TripleC*, *9*(1), 62–76. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84864790124&partnerID=tZOtx3y1

Ford, S. M. (2011). RECONCEPTUALIZING THE PUBLIC/PRIVATE DISTINCTION IN THE AGE OF INFORMATION TECHNOLOGY. *INFORMATION COMMUNICATION & SOCIETY*, *14*(4, SI), 550–567. http://doi.org/10.1080/1369118X.2011.562220

Fuchs, C. (2011). New Media, Web 2.0 and Surveillance. *Sociology Compass*, *5*(2), 134–147. http://doi.org/10.1111/j.1751-9020.2010.00354.x

Fuchs, C. (2012). The Political Economy of Privacy on Facebook. *Television & New Media*, *13*(2), 139–159. http://doi.org/10.1177/1527476411415699

Giroux, H. A. (2015). Totalitarian Paranoia in the Post-Orwellian Surveillance State. *CULTURAL STUDIES*, *29*(2), 108–140. http://doi.org/10.1080/09502386.2014.917118

Gurses, S., & Diaz, C. (2013). Two tales of privacy in online social networks. *IEEE Security & Privacy*, *11*(3), 29–37. http://doi.org/10.1109/MSP.2013.47

Humphreys, S. (2013). Predicting, securing and shaping the future: Mechanisms of governance in online social environments. *International Journal of Media & Cultural Politics*, *9*(3), 247–258. http://doi.org/10.1386/macp.9.3.247_1

Kang, J., Shilton, K., Estrin, D., Burke, J., & Hansen, M. (2012). Self-Surveillance Privacy. *IOWA LAW REVIEW*, *97*(3), 809–847. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84859056524&partnerID=tZOtx3y1

Kreissl, R. (2014). Assessing security technology's impact: old tools for new problems. *Science and Engineering Ethics*, *20*(3), 659–73. http://doi.org/10.1007/s11948-014-9529-9

Paliwala, A. (2013). Netizenship, security and freedom. *International Review of Law, Computers & Technology*, *27*(1-2), 104–123. http://doi.org/10.1080/13600869.2013.764139

Russett, P. C. (2011). A Contemporary Portrait of Information Privacy: Collective Communicative Consequences of Being Digital. *Review of Communication*, *11*(1), 39–50. http://doi.org/10.1080/15358593.2010.504882

Sevignani, S. (2012). The problem of privacy in capitalism and the alternative social networking site diaspora. *TripleC*, *10*(2), 600–617. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84861721442&partnerID=tZOtx3y1

Shroff, M., & Fordham, A. (2010). «Do you know who i am?» Exploring identity and privacy. *Information Polity*, *15*(4), 299–307. http://doi.org/10.3233/IP-2010-0162

Smith, C. A., Bellier, T., & Altick, J. (2011). Ego-Panopticism: The Evolution of Individual Power. *New Political Science*, *33*(1), 45–58. http://doi.org/10.1080/07393148.2011.544477

Van Otterlo, M. (2014). Automated experimentation in walden 3.0: The next step in profiling, predicting, control and surveillance. *Surveillance and Society*, *12*(2), 255–272. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84901052294&partnerID=tZOtx3y1

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *JOURNAL OF INFORMATION TECHNOLOGY*, *30*(1), 75–89. http://doi.org/10.1057/jit.2015.5

Arbete

12 artiklar

På ett övergripande plan visar artiklarna att övervakning av anställdas förehavanden på Internet är tämligen vanligt förekommande. T ex redovisar Alder et al. (2008) att så många som 63 procent av de amerikanska företagen övervakar sina anställdas internetanvänding. Samtidigt lyfts flera potentiellt skadliga effekter fram såsom minskad tillit till arbetsgivaren, motivation och arbetstillfredsställelse. Dock är sambanden inte helt enkla, utan i vilken mån övervakningen har en negativ effekt på de anställda är beroende av hur rättfärdigad den bedöms samt ett antal andra faktorer såsom anställningstid exempelvis.

Ball (2010) sätter frågan om övervakning av anställda i ett historiskt perspektiv och argumenterar för att fenomenet i sig inte är något nytt utan funnits länge. Dock har den digitala tekniken möjliggjort mer långtgående och djupgående möjligheter att i detalj följa de anställdas beteende. Vidare argumenteras det för att denna typ av digital övervakning potentiellt har konsekvenser för såväl anställdas hälsa och välmående som motivation och kreativitet.

Alder et al. (2006; 2008) visar att övervakning av anställdas internetanvändning kan påverka tilliten till arbetsgivaren negativt, vilket i sin tur även får konsekvenser för arbetstillfredsställelse, engagemang och vilja att stanna i företaget. Framförallt när det sker utan att samtycke inhämtats eller att syfte klargjorts.

Även Samaranayake och Gamage (2012) studerar anställdas upplevelser av och attityder till att övervakas i det digitala på arbetsplatsen. Deras främsta slutats är att upplevelsen av att vara övervakad påverkade arbetstillfredsställelsen på ett negativt sätt. ”Perceived Invasion of Privacy is negatively correlated to job satisfaction. Software professionals, who were worried about their privacy being violated because of electronic monitoring, were rather dissatisfied in their job.” (Samaranayake och Gamage 2012, s 242).

Dock visar en fördjupad analys att detta samband försvagas desto längre anställningstid de anställda hade. ”According to the regression model outputs developed based on the professional experience of the software professionals, the variation in job satisfaction explained by the independent variables decreased with higher professional experience. Also none of the variables were significant for the regression models developed for the groups of 10–15 years of experience and above 15 years of experience. This implies that the impact of electronic monitoring towards the job satisfaction becomes less significant with the maturity of the software professionals.” (Samaranayake och Gamage 2012, s 243). Samtidigt argumenteras det för att negativa upplevelser av övervakning kan förebyggas med information och tydliga policys. ”It is important that a policy for electronic monitoring exists at the

first place, and is communicated to all employees properly. This would effectively reduce the negative impacts of electronic monitoring associated with job satisfaction of the software professionals in Sri Lanka." (Samaranayake och Gamage 2012 s 243). Ett resonemang som ligger väl i linje med Adler et al. (2006).

Wen och Gershuny (2005) diskuterar de legala aspekterna av digital övervakning av anställda. På samma sätt som övriga artiklar som behandlar legala aspekter av övervakning och integritet i det digitala pekar de rättens svårighet att hänga med i den tekniska utvecklingen vilket innebär att skyddet för den enskilde anställde är svagt. I de fall ett ärende nått till rättegången har utfallet nästan alltid varit till arbetsgivarens favör. "Court decisions have supported employer monitoring of employees' email. Courts have even allowed the use of video cameras in employee changing rooms when the employer's objective was to prevent theft. Despite these favorable decisions, workplace privacy law in America is still in its infancy and gaps exist between the capability of the employer to monitor and the factual scenarios of the cases brought to court. For example, although monitoring employee website visits is a common practice, only a few cases have currently challenged its legitimacy" (Wen och Gershuny 2005, s 169). Avslutningsvis i artikeln argumenteras för vikten av att företagen utvecklar policys inom området. "companies need to develop computer-based monitoring policies for employees who have access to the Internet. It is also important to keep monitoring in perspective – it should not replace critical managerial skills and behaviors needed in the workplace." (Wen och Gershuny 2005, s 173).

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *INFORMATION & MANAGEMENT*, *43*(7), 894–903. http://doi.org/10.1016/j.im.2006.08.008

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2008). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *JOURNAL OF BUSINESS ETHICS*, *80*(3), 481–498. http://doi.org/10.1007/s10551-007-9432-2

Arlitt, M., Carlsson, N., Gill, P., Mahanti, A., & Williamson, C. (2011). Characterizing Intelligence Gathering and Control on an Edge Network. *ACM TRANSACTIONS ON INTERNET TECHNOLOGY*, *11*(1). http://doi.org/10.1145/1993083.1993085

Ball, K. (2010). Workplace surveillance: an overview. *LABOR HISTORY*, *51*(1), 87–106. http://doi.org/10.1080/00236561003654776

Chen, J. V., Chen, C. C., & Yang, H.-H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *INDUSTRIAL MANAGEMENT & DATA SYSTEMS*, *108*(1-2), 87–106. http://doi.org/10.1108/02635570810844106

Paschal, J. L., Stone, D. L., & Stone-Romero, E. F. (2009). Effects of electronic mail policies on invasiveness and fairness. *JOURNAL OF MANAGERIAL PSYCHOLOGY*, *24*(6), 502–525. http://doi.org/10.1108/02683940910974107

Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *TELEMATICS AND INFORMATICS*, *29*(2), 233–244. http://doi.org/10.1016/j.tele.2011.08.003

Searle, R. H. (2006). New technology: the potential impact of surveillance techniques in recruitment practices. *PERSONNEL REVIEW*, *35*(3), 336–351. http://doi.org/10.1108/00483480610656720

Van Gramberg, B., Teicher, J., & O'Rourke, A. (2014). Managing electronic communications: a new challenge for human resource managers. *INTERNATIONAL JOURNAL OF HUMAN RESOURCE MANAGEMENT*, *25*(16), 2234–2252. http://doi.org/10.1080/09585192.2013.872166

Wen, H. J., & Gershuny, P. (2005). Computer-based monitoring in the American workplace: Surveillance technologies and legal challenges. *Human Systems Management*. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-22344442448&partnerID=tZOtx3y1

Wen, H. J., Schwieger, D., & Gershuny, P. (2007). Internet usage monitoring in the workplace: Its legal challenges and implementation strategies. *INFORMATION SYSTEMS MANAGEMENT*, *24*(2), 185–196. http://doi.org/10.1080/10580530701221072

Whitty, M. T., & Carr, A. N. (2006). New rules in the workplace: Applying object-relations theory to explain problem Internet and email behaviour in the workplace. *COMPUTERS IN HUMAN BEHAVIOR*, *22*(2), 235–250. http://doi.org/10.1016/j.chb.2004.06.005

Kunskap och beteende bland unga

17 artiklar

Detta forskningsfält behandlar frågan om attityder till integritet på Internet (”Privacy perception/concerns”) relaterat till främst utbildning. I relation till detta diskuteras även frågor om socio-ekonomisk klasstillhörighet och skillnader i kunskapsnivåer (”Digital/privacy literacy”) samt olika pedagogiska grepp för att stärka individers kunskaper om Internet samt möjliggöra ett mer utvecklat säkerhetstänkande kring hur information hanteras i det digitala. Eller som Park (2013a, s. 3) uttrycker det: ” In short, to exercise appropriate measures of resistance against the potential abuse of personal data, it may be that users should be able to understand data flow in cyberspace and its acceptable limits of exposure” Park (2013b) pekar på stora skillnader i kunskapsnivåer och insikter i integritetsfrågor av internetanvändare vilka kan härledas till socio-ekonomisk status. I detta sammanhang uppmanas till särskilda riktade insatser mot utsatta grupper i syfte att jämna ut klasskillnader: ”Dissemination of personal information skill and knowledge is a salient issue in marginalized communities, as lacking the power to understand and resist surveillance can have negative consequences such as potential discrimination in one’s digital engagement.”(Park 2013b, s. 698).

Oulasvirta et al. (2014) visar att upplevd oro i förhållande till integritet i det digitala ökar när användare övervakas/kartläggs utan att avsändare och syfte är tydligt. Forskningsrojektet beskrivs enligt följande: ”An online experiment (n = 1,897) was carried out to understand how data disclosure practices in ubiquitous surveillance affect users’ privacy concerns. Information about the identity and intentions of a data collector was manipulated in hypothetical surveillance scenarios. Privacy concerns were found to differ across the scenarios and moderated by knowledge about the collector’s identity and intentions. Knowledge about intentions ex- hibited a stronger effect. When no information about intentions was disclosed, the respondents postulated negative intentions. A positive effect was found for disclosing neutral intentions of an organization or unknown data collector, but not for a private data collector. The findings underline the importance of disclosing intentions of data use to users in an easily understandable manner.” (Oulasvirta et al. 2014, s. 1). Följdaktligen gäller att transperans på ett signifikant sätt minskar förekomsten av oro. Utifrån detta konkluderas att: “The present findings underline that both the data collector’s identity and intention should be disclosed in such privacy nutrition labels. Furthermore, while exposing the two factors (identity and intention) will be beneficial, directing the user’s attention to the data collector’s intention will have a stronger effect than would drawing attention to identity alone.” (Oulasvirta et al. 2014, s. 5).

Berger et al. (2014) visar att ungdomars upplevelser av att vara övervakad på Internet kan leda till minskad nätanvändning: ”The findings indicate a significant quantitative decrease in Internet activity of users believing to be monitored.” (Berger et al. 2014).

Utbildning inom området behandlas i termer av ”E-safety education” och beskrivs på följande sätt: “E-safety refers to the way young people are taught about risks online, how they can protect themselves and to whom they should report worrying activity. Education is understood as one of a range of explicit strategies enacted by actors in the politics of digitally mediated surveillance.” (Barnard-Wills 2012, s. 240). Bakgrunden till behovet av riktade utbildningar kring E-safety riktat mot unga människor motiveras av gruppens särskilt utsatta ställning som såväl offer som gärninspersoner: Children are a population who are constructed as both potential victims and potential offenders in online settings. They are at risk from exposure to inappropriate media and from hostile actors. However they seek to circumvent restrictions on their behaviour, and can be responsible for harmful behaviour to each other in the form of cyber-bullying.” (Barnard-Wills 2012, s 248). Steeves och Regan (2014, s 299) beskriver ett antal olika initiativ till webbutbildningar riktade mot unga Internetanvändare: ”Educational programs typically reinforce this approach to privacy as informational control. For example, the European Union’s Ins@fe initiative, the myprivacy.mychoice.mylife (2013) campaign created by the Privacy Commissioner of Canada (2008) and the US government’s Kids.gov (2013) site all itemize the dangers associated with disclosing personal information online and encourage young people to limit what they say about themselves in online spaces. These sites advise young people that disclosing information opens them up predation and bullying; they link privacy – again defined as the non-disclosure of personal information – directly to safety.” Isasi-Andrieu et al. (2012) beskriver verktyget ”Gazela” vilket är avsett att hjälpa unga spanska Internetanvändare att bättre värdera och hantera intergritetsfrågor online.

Amos, C., Zhang, L., & Pentina, I. (2014). Investigating Privacy Perception and Behavior on Weibo. *JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING*, *26*(4), 43–56. http://doi.org/10.4018/joeuc.2014100103

Barnard-Wills, D. (2012). E-safety education: Young people, surveillance and responsibility. *CRIMINOLOGY & CRIMINAL JUSTICE*, *12*(3), 239–255. http://doi.org/10.1177/1748895811432957

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Isasi-Andrieu, A., Lopez-Carrera, A., & Ruiz-Ibanez, P. (2012). Gazela: social networks’ digital advisor for teenagers. *PROFESIONAL DE LA INFORMACION*, *21*(5), 514–519. http://doi.org/10.3145/epi.2012.sep.11

Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2014). *E-Business and Telecommunications*. (M. S. Obaidat & J. Filipe, Eds.)*Communications in Computer and Information Science* (Vol. 456). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-662-44788-8

Netchitailova, E. (2012). Facebook as a surveillance tool: From the perspective of the user. *TripleC*, *10*(2), 683–691. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84871454614&partnerID=tZOtx3y1

Orman, H. (2015). Why Won't Johnny Encrypt? *IEEE Internet Computing*, *19*(1), 90–94. http://doi.org/10.1109/MIC.2015.16

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 633–8. http://doi.org/10.1089/cyber.2013.0585

Park, Y. J. (2013a). Digital Literacy and Privacy Behavior Online. *COMMUNICATION RESEARCH*, *40*(2), 215–236. http://doi.org/10.1177/0093650211418338

Park, Y. J. (2013b). Offline Status, Online Status: Reproduction of Social Categories in Personal Information Skill and Knowledge. *SOCIAL SCIENCE COMPUTER REVIEW*, *31*(6), 680–702. http://doi.org/10.1177/0894439313485202

Park, Y. J., Jang, S. M., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *COMPUTERS IN HUMAN BEHAVIOR*, *38*, 296–303. http://doi.org/10.1016/j.chb.2014.05.041

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

Ross, J. (2011). Traces of self: online reflective practices and performances in higher education. *TEACHING IN HIGHER EDUCATION*, *16*(1), 113–126. http://doi.org/10.1080/13562517.2011.530753

Stančin, S., & Tomažič, S. (2010). User created content privacy or big brother is watching you. *Elektrotehniski Vestnik/Electrotechnical Review*, *77*(1), 5–12. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-77957199564&partnerID=tZOtx3y1

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313. http://doi.org/10.1108/JICES-01-2014-0004

Vickery, J. R. (2015). `I don't have anything to hide, but horizontal ellipsis `: the challenges and negotiations of social and mobile media privacy for non-dominant youth. *INFORMATION COMMUNICATION & SOCIETY*, *18*(3, SI), 281–294. http://doi.org/10.1080/1369118X.2014.989251

Hälsa

14 artiklar

En stor del av artiklarna inom detta område berör integritetsaspekter i relation till den ökade möjligheten att genom att följa nätanvändares digitala spår förutspå och intervenera för att stoppa smittspridning. Detta kan t.ex. ske genom verktyget ”Google trends”. Nuti et al. (2014) beskriver detta verktyg och dess potential på följande sätt: ”Google Trends analyzes a portion of the three billion daily Google Search searches and provides data on geospatial and temporal patterns in search volumes for user-specified terms. […]Google Trends holds potential as a free, easily accessible means to access large population search data to derive meaningful insights about population behavior and its link to health and health care.” (Nuti et al. 2014, s. 1 ff). Studien visar att Google trends står sig väl i relation till andra sätt att uppskatta och kartlägga hälsa och hälsobeteende. Trots möjligheterna som finns inbyggda i verktyget återstår dock arbete med utveckling: ”Google Trends could have been used to forecast the peak of scarlet fever in the UK 5 weeks before its arrival. Although studies are promising, strong correlations alone do not support the use of Google Trends for surveillance, and further work is needed to substantiate the reliability and real world applicability of Google Trends as a tool to monitor health-related phenomena.” (Nuti et al. 2014, s. 46). I relation till detta visar Gunn och Lester (2013) att sökningar på självmord kan vara ett bra sätt att på ett tidigt stadium fånga upp problemet och genomföra interventioner. Även Gu et al. (2014) visar att analyser av Internetsökningar kan vara ett bra sätt att tidigt kunna sätta in insatser vid epedemier. Cooper et al. (2005) argumenterar dock att det inte enbart är sjukdomsfallen i sig som genererar sökningar på Internet. I artikeln som behandlar cancer argumenterar de för att även mediaexponering av vissa sjukdomstillstånd tenderar att generera sökningar.

Gemensamt för de artiklar som behandlar möjligheterna att utifrån indivders digitala fotspår, i termer av sökningar (Cooper et al. 2005; Gunn och Lester 2013; Nuti et al. 2014;), blogginlägg (Gu et al. 2014), twitterflöden (Velardi et al. 2014), Facebooklikes (Gittelman et al. 2015) eller eget program som tankade ner information från flera olika källor på Internet (D’Ambrosio et al. 2015) är att de (förvånansvärt nog) överhuvudtaget inte behandlar integritetsfrågan alls utan enbart ser möjligheter med den digitala utvecklingen. Anledningen till att de kommit med i sökningen och gallringen är att begreppet ”Surveillance” förkommer flitigt. Men då enbart med innebörden: att genom insamling av data skaffa sig en god bild över ett fenomen.

Integritetsfrågan förekommer däremot tydligare när diskussionen rör digitalisering av den reguljära vården, vad gäller t ex elektronisk lagring och hantering av känslig personlig information. T ex skriver Kramer et al. (2012 , s. 7): ”The rapid proliferation of medical devices, and their growing sophistication, presents Internet-age challenges for multiple stakeholders. Without an understanding of security and privacy, it will be difficult for patients and clinicians to establish confidence in device safety and effectiveness.”

Även inom området e-hälsa (m-health eller e-health) finns en diskussion kring hanteringen av potentiellt integritetskänslig information (Lupton 2012; Lupton 2015). Särskilt då i relation data som genereras genom olika hälsoappar där användaren själv frivilligt mäter motionsvanor och anger andra typer av hälsobeteende som kost t.ex. Framförallt för Lupton resonemang kring hur fenomenet (att ständigt vara mätt och bedömd) påverkar vår självbild:

”Will the ‘nagging voices’ of the health-promoting messages automatically issuing forth from a person's mobile device be eventually ignored by its user? Or will these messages incite even greater feelings of guilt and shame at one's lack of self-control and self-discipline? Alternatively, will m-health technologies produce a cyborg, post-human self in which the routine collection of data about bodily actions and functions is simply incorporated unproblematically into the user's sense of selfhood and embodiment? How will concepts of ‘health’ itself be shaped and understood in a context in which one's biometric indicators may be constantly measured, analysed and displayed publicly on Facebook or Twitter? Will the ‘objective’ measurements offered by mobile devices take precedence over the ‘subjective’ assessments offered by the senses of the fleshly body?” (Lupton (2012, s. 242)

Boulos, M. N. K., Wheeler, S., Tavares, C., & Jones, R. (2011). How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *BIOMEDICAL ENGINEERING ONLINE*, *10*. http://doi.org/10.1186/1475-925X-10-24

Cooper, C. P., Mallon, K. P., Leadbetter, S., Pollack, L. A., & Peipins, L. A. (2005). Cancer Internet search activity on a major search engine, United States 2001-2003. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *7*(3). http://doi.org/10.2196/jmir.7.3.e36

Curtis, B. L. (2014). SOCIAL NETWORKING AND ONLINE RECRUITING FOR HIV RESEARCH: ETHICAL CHALLENGES. *JOURNAL OF EMPIRICAL RESEARCH ON HUMAN RESEARCH ETHICS*, *9*(1), 58–70. http://doi.org/10.1525/jer.2014.9.1.58

D’Ambrosio, A., Agricola, E., Russo, L., Gesualdo, F., Pandolfi, E., Bortolus, R., … Tozzi, A. E. (2015). Web-Based Surveillance of Public Information Needs for Informing Preconception Interventions. *PLOS ONE*, *10*(4). http://doi.org/10.1371/journal.pone.0122551

Davies, S. E. (2012). Nowhere to hide: informal disease surveillance networks tracing state behaviour. *Global Change, Peace & Security*, *24*(1), 95–107. http://doi.org/10.1080/14781158.2012.641272

Gittelman, S., Lange, V., Crawford, C. A. G., Okoro, C. A., Lieb, E., Dhingra, S. S., & Trimarchi, E. (2015). A New Source of Data for Public Health Surveillance: Facebook Likes. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *17*(4). http://doi.org/10.2196/jmir.3970

Gu, H. y, Chen, B., Zhu, H., Jiang, T., Wang, X., Chen, L., … Jiang, J. (2014). Importance of Internet Surveillance in Public Health Emergency Control and Prevention: Evidence From a Digital Epidemiologic Study During Avian Influenza A H7N9 Outbreaks. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *16*(1). http://doi.org/10.2196/jmir.2911

Gunn, J. F., & Lester, D. (2013). Using google searches on the internet to monitor suicidal behavior. *Journal of Affective Disorders*, *148*(2-3), 411–2. http://doi.org/10.1016/j.jad.2012.11.004

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLOS ONE*, *7*(7). http://doi.org/10.1371/journal.pone.0040200

Lupton, D. (2012). M-health and health promotion: The digital cyborg and surveillance society. *SOCIAL THEORY & HEALTH*, *10*(3), 229–244. http://doi.org/10.1057/sth.2012.6

Lupton, D. (2015). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–53. http://doi.org/10.1080/13691058.2014.920528

Myers, J., Frieden, T. R., Bherwani, K. M., & Henning, K. J. (2008). Privacy and public health at risk: Public health confidentiality in the digital age. *AMERICAN JOURNAL OF PUBLIC HEALTH*, *98*(5), 793–801. http://doi.org/10.2105/AJPH.2006.107706

Nuti, S. V, Wayda, B., Ranasinghe, I., Wang, S., Dreyer, R. P., Chen, S. I., & Murugiah, K. (2014). The Use of Google Trends in Health Care Research: A Systematic Review. *PLOS ONE*, *9*(10). http://doi.org/10.1371/journal.pone.0109583

Velardi, P., Stilo, G., Tozzi, A. E., & Gesualdo, F. (2014). Twitter mining for fine-grained syndromic surveillance. *Artificial Intelligence in Medicine*, *61*(3), 153–63. http://doi.org/10.1016/j.artmed.2014.01.002

Handel

12 artiklar

I centrum för artiklarna inom området handel är studiet av relationen mellan attityder till övervakning (privacy concerns) relaterat till köpbeteende (consumer behaviour) (Park et al. 2012; Park 2014). Resultaten mellan studierna spretar lite grand. T ex undersöker Park et al. (2012) huruvida oro för att integritetskänslig information skulle hamna i fel händer påverkar konsumenters beteende på Internet och kommer fram till: ”concern did not play a meaningful role in predicting the social dimension of privacy protection, such as avoiding certain web sites or falsifying information to hide one’s identity.” (Park et al. 2012, s. 1023-1024). Detta ligge i linje med Park (2014) som studerat huruvida det spelar någon roll i vilken mån en kommersiell hemsida tar hänsyn till hur integritetskänslig information hanteras i förhållande till antalet besökare till sidan. Med hanteringen av integritetskänslig information avses i detta fall om besökaren på hemsidan har möjlighet att styra vilken information denne delar med sig av. The central question is whether and to what extent the website interface is constructed as an enabler for informed choice in managing personal information. Here information privacy is defined as the ability to control one’s personal data and associated identities; widely regarded as one of the most vulnerable aspects of online use.” (Park 2014, s. 360-361). Som följande titel antyder, *A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites*, kan man inte förlita sig på att hänsynen till den personliga integriteten bland kommersiella aktörer ska öka genom att potentiella kunder väljer bort de aktörer som brister i detta hänseende. Detta då forskningen visar att möjligheten att påverka nivån på ”information privacy” inte spelar någon roll för konsumentbeteendet online. Forskningen beskrivs på följande sätt: ”This article examines user control of privacy online as indicated by functional features of commercial websites. While prior studies have focused on what’s written in privacy policy statements, systematic attention on the interactive aspects of the Web have been scant. This analysis, based on a sample of 398 commercial sites in the United States, shows that the more popular sites did not necessarily provide better privacy control features for users than sites that were randomly selected. In addition, there was no clear relationship between website characteristics and the functional features of privacy control.” (Park 2014, s. 360).

I oppossition till ovan hävdar Mercovic (2010) att frågor om hur integritet och hur personlig information hanteras visst spelar roll för konsumentbeteende och att företag som inte uppmärksammar detta faktum riskerar att förlora kunder. Dock formas, enligt artikelförfattaren, inte dessa uppfattningar så mycket av säkerhetsintställningar på enskilda hemsidor (som Park 2014 studerat ovan) utan snarare av organisationen bakom hemsidan.

I syfte att kunna förstå konsumenters vilja respektive ovilja att dela med sig av personlig information på Internet argumentera Li (2012)och Mekovic (2010) att vi måsta ta hänsyn till upplevd nytta med att göra så i relation till risk. Med andra ord handlar beslutet i slutändan inte enbart om tillit till organisationen eller en enskild hemsidas design och funktion; utan för att förstå konsumenters beteende online måste det vägas in upplevd nytta med att delge

personlig information. Li (2012) beskriver denna beräkning i termer av *calculus* (i.e., the trade-off between expected benefits and privacy risks).

Draper (2012) vänder sig mot bilden av att det är ”kundens inflytande/makt” som står i fokus vid datainsamling, eftersom kundens makt likställt med vad man beskriver som kundnytta. Kundnyttan beskrivs enligt följande: “…give you a more enjoyable, convenient shopping experience and to help us identify and/or provide information, products or services that may be of interest to you. The suggestion that personal data is used to help create a more relevant user experience may refer to the deals offered, the website content or the advertisements served.” (Draper 2012, s. 403). Istället handlar det om den ökade möjligheten att formulera riktade erbjudanden till kunder:” With the information these companies have about users, the ability to offer deals that are targeted based on an individual’s online reputation or profile (accurate or not) is immense.” (Draper 2012, s. 404). Och avslutar med: There is reason to be concerned about a business model that promotes the power of the consumer while simultaneously using information about that individual to create a unique consumer experience, the basis for which is beyond their control.” (Draper 2012, s. 405). Det som av företagen beskrivs som “kundens makt” handlar i praktiken om att skräddarsy reklam i syfte att maximera försäljning.

Draper, N. A. (2012). Group power: Discourses of consumer power and surveillance in group buying websites. *Surveillance and Society*, *9*(4), 394–407. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84873520765&partnerID=tZOtx3y1

Ghani, N. A., & Sidek, Z. M. (2009). Personal information privacy protection in e-commerce. *WSEAS Transactions on Information Science and Applications*, *6*(3), 407–416. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-66349109339&partnerID=tZOtx3y1

Humphreys, A. (2006). The Consumer as Foucauldian “Object of Knowledge.” *Social Science Computer Review*, *24*(3), 296–309. http://doi.org/10.1177/0894439306287975

Katos, V. (2012). An integrated model for online transactions: illuminating the black box. *Information Management & Computer Security*, *20*(3), 184–206. http://doi.org/10.1108/09685221211247299

L. Finn, R., & Wadhwa, K. (2014). The ethics of “smart” advertising and regulatory initiatives in the consumer intelligence industry. *Info*, *16*(3), 22–39. http://doi.org/10.1108/info-12-2013-0059

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *DECISION SUPPORT SYSTEMS*, *54*(1), 471–481. http://doi.org/10.1016/j.dss.2012.06.010

Mekovec, R. (2010). Online privacy: Overview and preliminary research. *Journal of Information and Organizational Sciences*. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-79960110760&partnerID=tZOtx3y1

Michael, M. G., Michael, K., & Perakslis, C. (2015). Überveillance, the web of things, and people: What is the culmination of all this surveillance? *IEEE Consumer Electronics Magazine*, *4*(2), 107–113. http://doi.org/10.1109/MCE.2015.2393007

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of `datification'. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, *24*(1), 3–14. http://doi.org/10.1016/j.jsis.2015.02.001

Park, Y. J. (2014). A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. *Policy & Internet*, *6*(4), 360–376. http://doi.org/10.1002/1944-2866.POI375

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027. http://doi.org/10.1016/j.chb.2012.01.004

Winter, J. S. (2014). Surveillance in ubiquitous network societies: normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. *ETHICS AND INFORMATION TECHNOLOGY*, *16*(1), 27–41. http://doi.org/10.1007/s10676-013-9332-3

Privata relationer

9 artiklar

Den digitala tekniken har inte enbart erbjudit ökade möjligheter för företag och stater att övervaka invidier. Detta sker även i enskilda privata relationer. Fokus här ligger framförallt på den möjighet att följa en partners eller före detta partners förehavanden på sociala medier. Det rör sig med andra ord inte om någon form av illegal verksamhet utan om en möjlighet att följa en annan persons digitala fotspår på Internet. Helsper och Whitty (2010) visar att det är tämligen vanligt att övervaka en (ex)partners digitala fotspår, såsom SMS, e-post och internethistorik: ”The findings show that there are surprisingly high levels of surveillance but that the types of surveillance used are quite limited. In around a third of the couples at least one person checked their partner’s emails or read their partner’s SMS messages without them knowing and in a fifth of the couples at least one of the partners had checked their spouse’s browser history.” (Helsper och Whitty 2010, s. 924).

Marshall (2012) har studerat hur tidigare partners hanterar sina relationer på Facebook post preakup, d.v.s. efter det att relatioen avslutats, samt vilka konsekvenser detta kan få för hälsa och välmående. Resultaten tyder på att de som vidhåller en vänskap på Facebook efter det att relationen avbrutits kan hindras i sin personliga mognad och förmåga att gå vidare i livet. Samtidigt uttrycker denna grupp, lite överaskande flera positiva aspketer: ”Contrary to expectations, people who remained Facebook friends with an ex-partner were lower in negative feelings, sexual desire, and longing for the former partner than people who were not Facebook friends.” (2012, s. 523). Detta i relation till Lukacs och Quan-Haase (2015) som mer entydigt visar att de som ägnar sig åt intesiv efterforskning av tidigare partners förehavanden på Facebook överlag upplever en högre grad av emotionellt lidande.

Även Tong (2013) har studerat övervakning av tidigare partners via Facebook och då med fokus på vilken information som eftersöks. Föga överaskande handlar det om sociala relationer, förekomsten av en eventuell ny partner, samt olika åsikter om den tidigare relationen. Samtidigt framkommer det tydligt att sociala normer avseende denna typ av övervakning spelar en viktigt roll: ”The correlationally based analyses indicate that the more the individuals apprehend the social disapproval associated with ex-partner surveillance, the less they engage in the behavior. They either interact directly with the ex-partner (a focus that was not deterred by concerns over network approval), or do not inquire at all. Or, individuals who care less about what others’ think may be using Facebook more than those who are concerned with social approval.” (Tong 2013, s. 792).

Denna typ av passiv insamling av data, som en tidigare partner frivilligt lämnar i sociala medier, drabbar som sagt mest den som själv samlar in datan. Dock finns fall där övervakningen gått längre och mer kommit att likna stalking. Chaulk och Jone (2011) beskriver flera olika sätt genom vilket Facebook kan användas i detta ändamål. T ex kan ex-partnerns

statusuppdateringar avslöja var denne kommer att befinna sig vid en viss tidpunkt: ”We find that offenders use Facebook to facilitate primary contact by providing information about where a target might be (e.g., at specific events advertised on Facebook, or showing up at locations mentioned by the target in their profile).” Det kan även röra sig om att skicka upprepade meddelanden till ex-partnern eller dennes vänner och familj, skicka virtuella presenter och inbjudningar eller skriva inlägg på ex-partnerns Facebook-sida. Även Grattagliano et al. (2012) skriver om stalking i det digitala och delar in beteendet i tre nivår där den tredje omfattar direkta hot: ”1) following (including showing up at the victim's home and workplace, maintaining surveillance, and setting up coincidences); 2) communicating (by telephone, mail, leaving notes, graffiti, gifts, e-mail, and internet); including the ordering of goods and services in the victim's name; 3) attacking or committing acts of violence (threats, direct harassment of the victim or of people close to the victim, damaging of personal goods, false accusations, physical or sexual violence).” (Grattagliano et al. 2012, s. 65).

Chaulk, K., & Jones, T. (2011). Online Obsessive Relational Intrusion: Further Concerns About Facebook. *Journal of Family Violence*, *26*(4), 245–254. http://doi.org/10.1007/s10896-011-9360-x

Fox, J., & Warber, K. M. (2014). Social Networking Sites in Romantic Relationships: Attachment, Uncertainty, and Partner Surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *17*(1), 3–7. http://doi.org/10.1089/cyber.2012.0667

Grattagliano, I., Cassibba, R., Greco, R., Laudisa, A., Torres, A., & Mastromarino, A. (2012). Stalking: old behaviour new crime. Reflections on 11 cases assessed in the judicial district of Bari. *RIVISTA DI PSICHIATRIA*, *47*(1), 65–72.

Gregg, M. (2013). Spousebusting: Intimacy, adultery, and surveillance technology. *Surveillance and Society*, *11*(3), 301–310. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84889685033&partnerID=tZOtx3y1

Helsper, E. J., & Whitty, M. T. (2010). Netiquette within married couples: Agreement about acceptable online behavior and surveillance between partners. *COMPUTERS IN HUMAN BEHAVIOR*, *26*(5), 916–926. http://doi.org/10.1016/j.chb.2010.02.006

Lukacs, V., & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. *INFORMATION COMMUNICATION & SOCIETY*, *18*(5, SI), 492–508. http://doi.org/10.1080/1369118X.2015.1008540

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior and Social Networking*, *15*(10), 521–6. http://doi.org/10.1089/cyber.2012.0125

McEwan, B. (2013). Sharing, caring, and surveilling: an actor-partner interdependence model examination of Facebook relational maintenance strategies. *Cyberpsychology, Behavior and Social Networking*, *16*(12), 863–9. http://doi.org/10.1089/cyber.2012.0717

Tong, S. T. (2013). Facebook use during relationship termination: uncertainty reduction and surveillance. *Cyberpsychology, Behavior and Social Networking*, *16*(11), 788–93. http://doi.org/10.1089/cyber.2012.0549

Mänskliga rättigheter i det digitala

4 artiklar

Den gemensamma problemställningen för dessa artiklar är relationen mellan å ena sidan enskilda staters behov och önksemål att förebygga hot mot medborgarana och å andra sidan problemet med att grundläggande mänskliga rättigheter åsidosätts när jakten på t.ex. terrorister hamnar i förgrunden. Självklart har denna problemställning en bakgrund i ”September 11” och den rättsliga reaktionen från Bushadminstrationen ”the USA Patriot act” som bland annat gav den amerikanska staten ett utökat mandat att övervaka individers kommunikation. McAdams(2005) formulerar spänningen mellan risk, säkerhet och grundläggande mänskliga rättigheter i en fråga: ”is the nature of the threat from transnational terrorism so great that it could permanently shift the balance between personal privacy and national security in the direction of the latter priority?” (McAdams 2005, s 480). I samma artikel konkluderas dock att oron kan vara obefogad: ”In short, there has not been a straightforward, causal relationship between the U.S. campaign against terrorism and the limitation of Fourth Amendment rights.” (McAdams 2005, s. 495).

Även O´Brien (2014) adresserar området risk, säkerhet och mänskliga rättigheter med fokus på den Australiensiska kontexten och hur barnens rättigheter tas tillvara. Ett problem som nämns här att risken (för tillexempel groming) övervärderas och att barnens egen förmåga att ta ställning till risker och hantera dessa undervärderas: ”Foremost amongst these is that welfare discourse homogenises children as passive victims, entirely lacking the skills to refuse advances from online predators. Contradicting this conception is the emerging body of evidence indicating that Australian children demonstrate discretion and significant critical literacy in negotiating online risks. Indeed, of the children who choose not to use social networking sites 23% chose not to do so because of concerns about cyber-safety.” (O´Brien 2014, s. 755-756). I relation till detta uppmanar författaren till att i större utsträckning se barn och unga som aktiva individer och inte som passiva objekt vars röster måste lyssnas till: ”Policy makers, legislators and educators must acknowledge the importance in balancing children’s rights to protection *and* autonomy. For children’s rights to be fully respected this balance *must* be relative to the evolving capacities of the child, and children *must* have the opportunity to contribute their voices to the policy agendas that will greatly effect them.” (O´Brien 2014, s. 771).

Hiranandani (2011) argumenterar för att terrorbegreppet är för inkludernade och missbrukas för att rättfärdiga långgående intrång i den personliga integriteten. I artikeln manas till ett ökat fokus på vikten att ta hänsyn till personlig integritet som en grundläggande mänsklig rättighet: ”The post-9/11 trend seems to be towards capitalising on fear while playing down the intrusive nature and repressive potential of surveillance and information technologies.97 Public awareness is key to create a shift in opinions about the potentially dangerous effects of new technologies given the lack of adequate protections to prevent their abuse. The power lies in public outcry and legislative/parliamentary action to demand transparency and accountability on part of the watchers.” (Hiranandani 2011, 1102).

Hankey, S., & O Clunaigh, D. (2013). Rethinking Risk and Security of Human Rights Defenders in the Digital Age. *Journal of Human Rights Practice*, *5*(3), 535–547. http://doi.org/10.1093/jhuman/hut023

McAdams, A. J. (2005). Internet surveillance after September 11 - Is the United States becoming Great Britain? *COMPARATIVE POLITICS*, *37*(4), 479+.

O'Brien, W. (2014). Australia's Digital Policy Agenda. *The International Journal of Children's Rights*, *22*(4), 748–775. http://doi.org/10.1163/15718182-02204004

Hiranandani, V. (2011). Privacy and security in the digital age: contemporary challenges and future directions. *The International Journal of Human Rights*, *15*(7), 1091–1106. http://doi.org/10.1080/13642987.2010.493360

Sousveillance

3 artiklar

Ett intressant begrepp i sammanhanget är ”Sousveillance” vilket kan beskrivas som en reaktion på den ökade övervakningen av individer från stater och företag. Begreppet kan knytas till begreppet Ego-Panopticism som diskuterades i avsnittet om generella teoretiska resonemang ovan. Grundtanken med Sousveillance är att vända på kikaren så att övervakaren blir den övervakade. Här skapar övervakning och intrång i den personliga integriteten en reaktion och nya beteenden vilka tar sig yttryck i att medborgare med hjälp av digital teknik utsätter makthavare för övervakning. Fernback (2013, s. 11) beskriver det som ”Sousveillance is "watching from below," a form of inverse surveillance in which people monitor the surveillors. Examples include citizen video, watchdog web sites, or the monitoring of authorities (corporations, military, government). Sousveillance embraces the idea of transparency as an antidote to concentrated power in the hands of surveillors.” Exempel på medel och forum som kan användas i detta syfte är diskussionsgrupper på Facebook (intressant nog mest riktade mot forumet som används. T ex gruppen *Petition: Facebook, Stop Invading My Privacy*) (Fernback 2013), digitalt samordnad produktion och spridning av videofilmer av polisövervåld (Bradshaw (2013) och spridning av, för polisen kompromenterande, övervakningsfilmer som ljudfiler (Ganascia 2010).

Förhoppningar och utmaningar inför framtiden: ”While the potential remains for sousveillance to assist global justice activists in challenging authority and seeking alternative solutions to neoliberal globalization, an emancipatory relationship to social media and digital communication technologies is something that is not given, but must be critically and continuously forged. (Braadshaw 2013, s. 410)

Bradshaw, E. A. (2013). This is What a Police State Looks Like: Sousveillance, Direct Action and the Anti-corporate Globalization Movement. *CRITICAL CRIMINOLOGY*, *21*(4), 447–461. http://doi.org/10.1007/s10612-013-9205-4

Fernback, J. (2013). Sousveillance: Communities of resistance to the surveillance environment. *Telematics and Informatics*, *30*(1), 11–21. http://doi.org/10.1016/j.tele.2012.03.003

Ganascia, J.-G. (2010). The generalized sousveillance society. *Social Science Information*, *49*(3), 489–507. http://doi.org/10.1177/0539018410371027

Övrigt

5 artiklar

Här rymms artiklar som inte riktigt passade in under någon annan kategori. Bland annat en artikel som introducerar begreppet ”Cyber-Paranoia” vilket beskriver ett tillstånd av obefogad skräck för hot på Internet hos individer (Mason et al. 2014).

Garnar (2012) behandlar frågan med missbruk av offentliga datorer och därmed behovet av att begränsa och övervaka användningen.

Park et al. (2015) beskriver ett antal personlighetstyper relaterat till konsumentbeteende på Internet.

Lin och Lo (20105) beskriver ett nytt sätt för datainsamling av trafikdata på motorvägar och potentiella integritetsfrågor i relation till detta.

Andrejevic, M. (2007). Ubiquitous computing and the digital enclosure movement. *MEDIA INTERNATIONAL AUSTRALIA*, (125), 106–117.

Garnar, M. L. (2012). For the Sake of One Child. *Journal of Information Ethics*, *21*(1), 12–20. http://doi.org/10.3172/JIE.21.1.12

Lin, W.-H., & Lo, H. K. (2015). Highway voting system: Embracing a possible paradigm shift in traffic data acquisition. *Transportation Research Part C: Emerging Technologies*, *56*, 149–160. http://doi.org/10.1016/j.trc.2015.03.025

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *FRONTIERS IN PSYCHOLOGY*, *5*. http://doi.org/10.3389/fpsyg.2014.01298

Park, M.-S., Shin, J.-K., & Ju, Y. (2015). A Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. *PSYCHOLOGY & MARKETING*, *32*(6), 601–610. http://doi.org/10.1002/mar.20803

Beteende

Det finns frågor som griper in i flera områden och som inte har någon direkt koppling till ett specifikt fält. En sådan generell fråga rör kopplingen mellan hur den digitala tekniken och möjligheten/hotet att övervaka/övervakas påverkar beteende. Berger et al. (2014) hävdar i artikeln *Surveillance in Digital Space and Changes in User Behaviour* att frågan är dåligt beforskad och skriver att ”the social consequences of a comprehensive surveillance like altering the individual behavior in the digital space have hardly been studied.” I studien som är berördes under rubriken ”Kunskap och beteende bland unga” studeras beteende i termer av nätanvändande och det konkluderas att risken för övervakning medför ett minskat internetanvändande.

En annan artikel (Fuchs 2010) som rör samma område argumenterar för att ökad information och kunskapsbildning för unga angående integritetsfrågor på Internet bidrar till vad som benämns som ”critical information behaviour”. Ett begrepp som definieras som: ”Critical information behaviour involves actions that question the status quo of information systems, it asks if the users really benefit from the standard settings of these systems, and which changes need to be undertaken in order to overcome or lessen power differentials.” (Fuchs 2010, s. 180).

Artikeln *Privacy behaviors after Snowden* (Preibusch 2015) visar att ”privacy beahaviours” visserligen ökade efter Edward Snowdens avslöjande om den långtgående statliga övervakningen som skedde inom ramen för programmet PRISM, men att ökningen var tämligen marginell och inte varade särskilt länge: ”I combined high-resolution data from primary sources that indicate the new public information on PRISM led to momentarily increased interest in privacy and protection. However, the spike was much less than for other news events (such as the royal baby and the U.S. Open golf tournament). It was also less than the increased interest following the removal of privacyenhancing functions in Facebook, Android, and Gmail. While media coverage of PRISM and surveillance was elevated for the 30 weeks following PRISM day, many privacy behaviors faded quickly. Visits to Microsoft’s corporate privacy policy page stayed high, but only certain privacy-related webpages kept larger audiences—those on Snowden and surveillance—while Wikipedia articles about PRISM topics lost their increased readership. Snowden’s revelations brought few new users to privacy-enhancing technologies” (Preibusch 2015, s. 55).

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

4. Artiklar vilka byger på empiriska studier indelade utifrån metod

Vilar mot empiriska studier

Av de sammanlagt 172 artiklarna som ingår i den systematiska litteraturöversikten vilar 56 stycken på empirisk grund, i meningen att det dras slutsatser i artikeln på basis av en systematisk insamling och analys av data. Det ska dock nämnas att det inte varit helt enkelt att göra denna distinktion. Många av artiklarna som inte bedömts ”vila på empirisk grund” redovisar t ex en specifik teknik tämligen ingående (se t ex Lupton 2015) alt. konsekvenser av en specifik lagstiftning för integritet (se t ex Konstadinides 2011) men har inte bedömts presentera ett resultat som bygger på slutsatser av en analys som genomförts av empirin. Vidare bygger många av de artiklar vilka inte har skrivits utifrån egen empiri på tidigare forskning vilken är empirisk. Av de artiklar som vilar på egen empirisk grund har de lite olika angreppssätt för insamling av data. Följande angreppssätt har urskilts och används för att dela upp artiklarna: survey, intervjuer, case studies, mixed methods, dokumentanalys, Internetloggar, experimentella metoder samt övrigt.

Survey 25 st

Amos, C., Zhang, L., & Pentina, I. (2014). Investigating Privacy Perception and Behavior on Weibo. *JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING*, *26*(4), 43–56. http://doi.org/10.4018/joeuc.2014100103

Best, S. J., & Krueger, B. S. (2008). Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms. *Journal of Information Technology & Politics*, *5*(2), 191–212. http://doi.org/10.1080/19331680802294479

Budak, J., Anic, I.-D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *INNOVATION-THE EUROPEAN JOURNAL OF SOCIAL SCIENCE RESEARCH*, *26*(1-2, SI), 100–118. http://doi.org/10.1080/13511610.2013.723404

Budak, J., Rajh, E., & Anic, I.-D. (2015). Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens. *JOURNAL OF BALKAN AND NEAR EASTERN STUDIES*, *17*(1), 29–48. http://doi.org/10.1080/19448953.2014.990278

Chaulk, K., & Jones, T. (2011). Online Obsessive Relational Intrusion: Further Concerns About Facebook. *Journal of Family Violence*, *26*(4), 245–254. http://doi.org/10.1007/s10896-011-9360-x

Chen, J. V., Chen, C. C., & Yang, H.-H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *INDUSTRIAL MANAGEMENT & DATA SYSTEMS*, *108*(1-2), 87–106. http://doi.org/10.1108/02635570810844106

Cohrs, J. C., Kielmann, S., Maes, J., & Moschner, B. (2005). Effects of Right-Wing Authoritarianism and Threat from Terrorism on Restriction of Civil Liberties. *Analyses of Social Issues and Public Policy*, *5*(1), 263–276. http://doi.org/10.1111/j.1530-2415.2005.00071.x

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Internet users’ privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *JOURNAL OF GLOBAL INFORMATION MANAGEMENT*, *14*(4), 57–93. http://doi.org/10.4018/jgim.2006100103

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, *17*(3), 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Fox, J., & Warber, K. M. (2014). Social Networking Sites in Romantic Relationships: Attachment, Uncertainty, and Partner Surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *17*(1), 3–7. http://doi.org/10.1089/cyber.2012.0667

Helsper, E. J., & Whitty, M. T. (2010). Netiquette within married couples: Agreement about acceptable online behavior and surveillance between partners. *COMPUTERS IN HUMAN BEHAVIOR*, *26*(5), 916–926. http://doi.org/10.1016/j.chb.2010.02.006

Kang, S., & Gearhart, S. (2010). E-Government and Civic Engagement: How is Citizens' Use of City Web Sites Related with Civic Involvement and Political Behaviors? *JOURNAL OF BROADCASTING & ELECTRONIC MEDIA*, *54*(3), 443–462. http://doi.org/10.1080/08838151.2010.498847

Katos, V. (2012). An integrated model for online transactions: illuminating the black box. *Information Management & Computer Security*, *20*(3), 184–206. http://doi.org/10.1108/09685221211247299

Krueger, B. S. (2005). Government surveillance and political participation on the Internet. *SOCIAL SCIENCE COMPUTER REVIEW*, *23*(4), 439–452. http://doi.org/10.1177/0894439305278871

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior and Social Networking*, *15*(10), 521–6. http://doi.org/10.1089/cyber.2012.0125

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *FRONTIERS IN PSYCHOLOGY*, *5*. http://doi.org/10.3389/fpsyg.2014.01298

Park, M.-S., Shin, J.-K., & Ju, Y. (2015). A Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. *PSYCHOLOGY & MARKETING*, *32*(6), 601–610. http://doi.org/10.1002/mar.20803

Park, Y. J. (2013a). Digital Literacy and Privacy Behavior Online. *COMMUNICATION RESEARCH*, *40*(2), 215–236. http://doi.org/10.1177/0093650211418338

Park, Y. J. (2013b). Offline Status, Online Status: Reproduction of Social Categories in Personal Information Skill and Knowledge. *SOCIAL SCIENCE COMPUTER REVIEW*, *31*(6), 680–702. http://doi.org/10.1177/0894439313485202

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027. http://doi.org/10.1016/j.chb.2012.01.004

Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *TELEMATICS AND INFORMATICS*, *29*(2), 233–244. http://doi.org/10.1016/j.tele.2011.08.003

Smith, E., & Lyon, D. (2013). Comparison of survey findings from Canada and the USA on surveillance and privacy from 2006 and 2012. *Surveillance and Society*, *11*(1-2), 190–203. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84881272799&partnerID=tZOtx3y1

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313. http://doi.org/10.1108/JICES-01-2014-0004

Tong, S. T. (2013). Facebook use during relationship termination: uncertainty reduction and surveillance. *Cyberpsychology, Behavior and Social Networking*, *16*(11), 788–93. http://doi.org/10.1089/cyber.2012.0549

Xu, H., & Dinev, T. (2012). The security-liberty balance: individuals' attitudes towards internet government surveillance. *Electronic Government, an International Journal*, *9*(1), 46. http://doi.org/10.1504/EG.2012.044778

Intervju 4 st

Draper, N. A. (2012). Group power: Discourses of consumer power and surveillance in group buying websites. *Surveillance and Society*, *9*(4), 394–407. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84873520765&partnerID=tZOtx3y1

Ebenger, T. (2008). The USA PATRIOT Act: Implications for Private E-Mail. *Journal of Information Technology & Politics*, *4*(4), 47–64. http://doi.org/10.1080/19331680801978759

Kim, H., Giacomin, J., & Macredie, R. (2014). A Qualitative Study of Stakeholders' Perspectives on the Social Network Service Environment. *International Journal of Human-Computer Interaction*, *30*(12), 965–976. http://doi.org/10.1080/10447318.2014.925383

Vickery, J. R. (2015). `I don't have anything to hide, but horizontal ellipsis `: the challenges and negotiations of social and mobile media privacy for non-dominant youth. *INFORMATION COMMUNICATION & SOCIETY*, *18*(3, SI), 281–294. http://doi.org/10.1080/1369118X.2014.989251

Case study 4 st

E-safety education: Young people, surveillance and responsibilityBarnard-Wills, D. (2012). E-safety education: Young people, surveillance and responsibility. *CRIMINOLOGY & CRIMINAL JUSTICE*, *12*(3), 239–255. http://doi.org/10.1177/1748895811432957

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Jiang, M., & Okamoto, K. (2014). National Identity, Ideological Apparatus, or Panopticon? A Case Study of the Chinese National Search Engine Jike. *Policy & Internet*, *6*(1), 89–107. http://doi.org/10.1002/1944-2866.POI353

Nuti, S. V, Wayda, B., Ranasinghe, I., Wang, S., Dreyer, R. P., Chen, S. I., & Murugiah, K. (2014). The Use of Google Trends in Health Care Research: A Systematic Review. *PLOS ONE*, *9*(10). http://doi.org/10.1371/journal.pone.0109583

Mixed method 3 st

Lukacs, V., & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. *INFORMATION COMMUNICATION & SOCIETY*, *18*(5, SI), 492–508. http://doi.org/10.1080/1369118X.2015.1008540

Park, Y. J., Jang, S. M., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *COMPUTERS IN HUMAN BEHAVIOR*, *38*, 296–303. http://doi.org/10.1016/j.chb.2014.05.041

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. a. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129–141. http://doi.org/10.1016/j.giq.2015.01.003

Dokumentanalys 2 st

Farinosi, M. (2011). Deconstructing bentham's panopticon: The new metaphors of surveillance in the web 2.0 environment. *TripleC*, *9*(1), 62–76. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84864790124&partnerID=tZOtx3y1

Haikola, S., & Jonsson, S. (2007). State surveillance on the internet - The Swedish debate and the future role of libraries and LIS. *LIBRI*, *57*(4), 209–218. http://doi.org/10.1515/LIBR.2007.209

Internetloggar 13 st

Arlitt, M., Carlsson, N., Gill, P., Mahanti, A., & Williamson, C. (2011). Characterizing Intelligence Gathering and Control on an Edge Network. *ACM TRANSACTIONS ON INTERNET TECHNOLOGY*, *11*(1). http://doi.org/10.1145/1993083.1993085

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Government surveillance disclosures, bilateral trust and Indonesia-Australia cross-border security cooperation: Social network analysis of Twitter data. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 118–128. http://doi.org/10.1016/j.giq.2015.01.002

Cooper, C. P., Mallon, K. P., Leadbetter, S., Pollack, L. A., & Peipins, L. A. (2005). Cancer Internet search activity on a major search engine, United States 2001-2003. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *7*(3). http://doi.org/10.2196/jmir.7.3.e36

D'Ambrosio, A., Agricola, E., Russo, L., Gesualdo, F., Pandolfi, E., Bortolus, R., … Tozzi, A. E. (2015). Web-Based Surveillance of Public Information Needs for Informing Preconception Interventions. *PLOS ONE*, *10*(4). http://doi.org/10.1371/journal.pone.0122551

Gittelman, S., Lange, V., Crawford, C. A. G., Okoro, C. A., Lieb, E., Dhingra, S. S., & Trimarchi, E. (2015). A New Source of Data for Public Health Surveillance: Facebook Likes. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *17*(4). http://doi.org/10.2196/jmir.3970

Gu, H. y, Chen, B., Zhu, H., Jiang, T., Wang, X., Chen, L., … Jiang, J. (2014). Importance of Internet Surveillance in Public Health Emergency Control and Prevention: Evidence From a Digital Epidemiologic Study During Avian Influenza A H7N9 Outbreaks. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *16*(1). http://doi.org/10.2196/jmir.2911

Gunn, J. F., & Lester, D. (2013). Using google searches on the internet to monitor suicidal behavior. *Journal of Affective Disorders*, *148*(2-3), 411–2. http://doi.org/10.1016/j.jad.2012.11.004

Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2014). *E-Business and Telecommunications*. (M. S. Obaidat & J. Filipe, Eds.)*Communications in Computer and Information Science* (Vol. 456). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-662-44788-8

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLOS ONE*, *7*(7). http://doi.org/10.1371/journal.pone.0040200

McEwan, B. (2013). Sharing, caring, and surveilling: an actor-partner interdependence model examination of Facebook relational maintenance strategies. *Cyberpsychology, Behavior and Social Networking*, *16*(12), 863–9. http://doi.org/10.1089/cyber.2012.0717

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

Velardi, P., Stilo, G., Tozzi, A. E., & Gesualdo, F. (2014). Twitter mining for fine-grained syndromic surveillance. *Artificial Intelligence in Medicine*, *61*(3), 153–63. http://doi.org/10.1016/j.artmed.2014.01.002

Experiment 4 st

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *INFORMATION & MANAGEMENT*, *43*(7), 894–903. http://doi.org/10.1016/j.im.2006.08.008

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2008). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *JOURNAL OF BUSINESS ETHICS*, *80*(3), 481–498. http://doi.org/10.1007/s10551-007-9432-2

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 633–8. http://doi.org/10.1089/cyber.2013.0585

Paschal, J. L., Stone, D. L., & Stone-Romero, E. F. (2009). Effects of electronic mail policies on invasiveness and fairness. *JOURNAL OF MANAGERIAL PSYCHOLOGY*, *24*(6), 502–525. http://doi.org/10.1108/02683940910974107

Övrigt 1 st

Park, Y. J. (2014). A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. *Policy & Internet*, *6*(4), 360–376. http://doi.org/10.1002/1944-2866.POI375

Samtliga 56 st

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *INFORMATION & MANAGEMENT*, *43*(7), 894–903. http://doi.org/10.1016/j.im.2006.08.008

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2008). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *JOURNAL OF BUSINESS ETHICS*, *80*(3), 481–498. http://doi.org/10.1007/s10551-007-9432-2

Amos, C., Zhang, L., & Pentina, I. (2014). Investigating Privacy Perception and Behavior on Weibo. *JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING*, *26*(4), 43–56. http://doi.org/10.4018/joeuc.2014100103

Arlitt, M., Carlsson, N., Gill, P., Mahanti, A., & Williamson, C. (2011). Characterizing Intelligence Gathering and Control on an Edge Network. *ACM TRANSACTIONS ON INTERNET TECHNOLOGY*, *11*(1). http://doi.org/10.1145/1993083.1993085

Berger, P. A., Brumme, R., Cap, C. H., & Otto, D. (2014). Surveillance in Digital Space and Changes in User Behaviour. *SOZIALE WELT-ZEITSCHRIFT FUR SOZIALWISSENSCHAFTLICHE FORSCHUNG UND PRAXIS*, *65*(2), 221+.

Best, S. J., & Krueger, B. S. (2008). Political Conflict and Public Perceptions of Government Surveillance on the Internet: An Experiment of Online Search Terms. *Journal of Information Technology & Politics*, *5*(2), 191–212. http://doi.org/10.1080/19331680802294479

Budak, J., Anic, I.-D., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *INNOVATION-THE EUROPEAN JOURNAL OF SOCIAL SCIENCE RESEARCH*, *26*(1-2, SI), 100–118. http://doi.org/10.1080/13511610.2013.723404

Budak, J., Rajh, E., & Anic, I.-D. (2015). Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens. *JOURNAL OF BALKAN AND NEAR EASTERN STUDIES*, *17*(1), 29–48. http://doi.org/10.1080/19448953.2014.990278

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Government surveillance disclosures, bilateral trust and Indonesia-Australia cross-border security cooperation: Social network analysis of Twitter data. *GOVERNMENT INFORMATION QUARTERLY*, *32*(2), 118–128. http://doi.org/10.1016/j.giq.2015.01.002

Chaulk, K., & Jones, T. (2011). Online Obsessive Relational Intrusion: Further Concerns About Facebook. *Journal of Family Violence*, *26*(4), 245–254. http://doi.org/10.1007/s10896-011-9360-x

Chen, J. V., Chen, C. C., & Yang, H.-H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *INDUSTRIAL MANAGEMENT & DATA SYSTEMS*, *108*(1-2), 87–106. http://doi.org/10.1108/02635570810844106

Cohrs, J. C., Kielmann, S., Maes, J., & Moschner, B. (2005). Effects of Right-Wing Authoritarianism and Threat from Terrorism on Restriction of Civil Liberties. *Analyses of Social Issues and Public Policy*, *5*(1), 263–276. http://doi.org/10.1111/j.1530-2415.2005.00071.x

Cooper, C. P., Mallon, K. P., Leadbetter, S., Pollack, L. A., & Peipins, L. A. (2005). Cancer Internet search activity on a major search engine, United States 2001-2003. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *7*(3). http://doi.org/10.2196/jmir.7.3.e36

D'Ambrosio, A., Agricola, E., Russo, L., Gesualdo, F., Pandolfi, E., Bortolus, R., … Tozzi, A. E. (2015). Web-Based Surveillance of Public Information Needs for Informing Preconception Interventions. *PLOS ONE*, *10*(4). http://doi.org/10.1371/journal.pone.0122551

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *JOURNAL OF GLOBAL INFORMATION MANAGEMENT*, *14*(4), 57–93. http://doi.org/10.4018/jgim.2006100103

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *JOURNAL OF STRATEGIC INFORMATION SYSTEMS*, *17*(3), 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Draper, N. A. (2012). Group power: Discourses of consumer power and surveillance in group buying websites. *Surveillance and Society*, *9*(4), 394–407. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84873520765&partnerID=tZOtx3y1

E-safety education: Young people, surveillance and responsibilityBarnard-Wills, D. (2012). E-safety education: Young people, surveillance and responsibility. *CRIMINOLOGY & CRIMINAL JUSTICE*, *12*(3), 239–255. http://doi.org/10.1177/1748895811432957

Ebenger, T. (2008). The USA PATRIOT Act: Implications for Private E-Mail. *Journal of Information Technology & Politics*, *4*(4), 47–64. http://doi.org/10.1080/19331680801978759

Farinosi, M. (2011). Deconstructing bentham's panopticon: The new metaphors of surveillance in the web 2.0 environment. *TripleC*, *9*(1), 62–76. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84864790124&partnerID=tZOtx3y1

Fox, J., & Warber, K. M. (2014). Social Networking Sites in Romantic Relationships: Attachment, Uncertainty, and Partner Surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *17*(1), 3–7. http://doi.org/10.1089/cyber.2012.0667

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171–185. http://doi.org/10.1007/s10676-010-9220-z

Gittelman, S., Lange, V., Crawford, C. A. G., Okoro, C. A., Lieb, E., Dhingra, S. S., & Trimarchi, E. (2015). A New Source of Data for Public Health Surveillance: Facebook Likes. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *17*(4). http://doi.org/10.2196/jmir.3970

Gu, H. y, Chen, B., Zhu, H., Jiang, T., Wang, X., Chen, L., … Jiang, J. (2014). Importance of Internet Surveillance in Public Health Emergency Control and Prevention: Evidence From a Digital Epidemiologic Study During Avian Influenza A H7N9 Outbreaks. *JOURNAL OF MEDICAL INTERNET RESEARCH*, *16*(1). http://doi.org/10.2196/jmir.2911

Gunn, J. F., & Lester, D. (2013). Using google searches on the internet to monitor suicidal behavior. *Journal of Affective Disorders*, *148*(2-3), 411–2. http://doi.org/10.1016/j.jad.2012.11.004

Haikola, S., & Jonsson, S. (2007). State surveillance on the internet - The Swedish debate and the future role of libraries and LIS. *LIBRI*, *57*(4), 209–218. http://doi.org/10.1515/LIBR.2007.209

Helsper, E. J., & Whitty, M. T. (2010). Netiquette within married couples: Agreement about acceptable online behavior and surveillance between partners. *COMPUTERS IN HUMAN BEHAVIOR*, *26*(5), 916–926. http://doi.org/10.1016/j.chb.2010.02.006

Jiang, M., & Okamoto, K. (2014). National Identity, Ideological Apparatus, or Panopticon? A Case Study of the Chinese National Search Engine Jike. *Policy & Internet*, *6*(1), 89–107. http://doi.org/10.1002/1944-2866.POI353

Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2014). *E-Business and Telecommunications*. (M. S. Obaidat & J. Filipe, Eds.)*Communications in Computer and Information Science* (Vol. 456). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-662-44788-8

Kang, S., & Gearhart, S. (2010). E-Government and Civic Engagement: How is Citizens' Use of City Web Sites Related with Civic Involvement and Political Behaviors? *JOURNAL OF BROADCASTING & ELECTRONIC MEDIA*, *54*(3), 443–462. http://doi.org/10.1080/08838151.2010.498847

Katos, V. (2012). An integrated model for online transactions: illuminating the black box. *Information Management & Computer Security*, *20*(3), 184–206. http://doi.org/10.1108/09685221211247299

Kim, H., Giacomin, J., & Macredie, R. (2014). A Qualitative Study of Stakeholders' Perspectives on the Social Network Service Environment. *International Journal of Human-Computer Interaction*, *30*(12), 965–976. http://doi.org/10.1080/10447318.2014.925383

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLOS ONE*, *7*(7). http://doi.org/10.1371/journal.pone.0040200

Krueger, B. S. (2005). Government surveillance and political participation on the Internet. *SOCIAL SCIENCE COMPUTER REVIEW*, *23*(4), 439–452. http://doi.org/10.1177/0894439305278871

Lukacs, V., & Quan-Haase, A. (2015). Romantic breakups on Facebook: new scales for studying post-breakup behaviors, digital distress, and surveillance. *INFORMATION COMMUNICATION & SOCIETY*, *18*(5, SI), 492–508. http://doi.org/10.1080/1369118X.2015.1008540

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior and Social Networking*, *15*(10), 521–6. http://doi.org/10.1089/cyber.2012.0125

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *FRONTIERS IN PSYCHOLOGY*, *5*. http://doi.org/10.3389/fpsyg.2014.01298

McEwan, B. (2013). Sharing, caring, and surveilling: an actor-partner interdependence model examination of Facebook relational maintenance strategies. *Cyberpsychology, Behavior and Social Networking*, *16*(12), 863–9. http://doi.org/10.1089/cyber.2012.0717

Nuti, S. V, Wayda, B., Ranasinghe, I., Wang, S., Dreyer, R. P., Chen, S. I., & Murugiah, K. (2014). The Use of Google Trends in Health Care Research: A Systematic Review. *PLOS ONE*, *9*(10). http://doi.org/10.1371/journal.pone.0109583

Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 633–8. http://doi.org/10.1089/cyber.2013.0585

Park, M.-S., Shin, J.-K., & Ju, Y. (2015). A Taxonomy of Social Networking Site Users: Social Surveillance and Self-surveillance Perspective. *PSYCHOLOGY & MARKETING*, *32*(6), 601–610. http://doi.org/10.1002/mar.20803

Park, Y. J. (2013a). Digital Literacy and Privacy Behavior Online. *COMMUNICATION RESEARCH*, *40*(2), 215–236. http://doi.org/10.1177/0093650211418338

Park, Y. J. (2013b). Offline Status, Online Status: Reproduction of Social Categories in Personal Information Skill and Knowledge. *SOCIAL SCIENCE COMPUTER REVIEW*, *31*(6), 680–702. http://doi.org/10.1177/0894439313485202

Park, Y. J. (2014). A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites. *Policy & Internet*, *6*(4), 360–376. http://doi.org/10.1002/1944-2866.POI375

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior*, *28*(3), 1019–1027. http://doi.org/10.1016/j.chb.2012.01.004

Park, Y. J., Jang, S. M., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *COMPUTERS IN HUMAN BEHAVIOR*, *38*, 296–303. http://doi.org/10.1016/j.chb.2014.05.041

Paschal, J. L., Stone, D. L., & Stone-Romero, E. F. (2009). Effects of electronic mail policies on invasiveness and fairness. *JOURNAL OF MANAGERIAL PSYCHOLOGY*, *24*(6), 502–525. http://doi.org/10.1108/02683940910974107

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM*, *58*(5), 48–55. http://doi.org/10.1145/2663341

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. a. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129–141. http://doi.org/10.1016/j.giq.2015.01.003

Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *TELEMATICS AND INFORMATICS*, *29*(2), 233–244. http://doi.org/10.1016/j.tele.2011.08.003

Smith, E., & Lyon, D. (2013). Comparison of survey findings from Canada and the USA on surveillance and privacy from 2006 and 2012. *Surveillance and Society*, *11*(1-2), 190–203. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84881272799&partnerID=tZOtx3y1

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298–313. http://doi.org/10.1108/JICES-01-2014-0004

Tong, S. T. (2013). Facebook use during relationship termination: uncertainty reduction and surveillance. *Cyberpsychology, Behavior and Social Networking*, *16*(11), 788–93. http://doi.org/10.1089/cyber.2012.0549

Velardi, P., Stilo, G., Tozzi, A. E., & Gesualdo, F. (2014). Twitter mining for fine-grained syndromic surveillance. *Artificial Intelligence in Medicine*, *61*(3), 153–63. http://doi.org/10.1016/j.artmed.2014.01.002

Vickery, J. R. (2015). `I don't have anything to hide, but horizontal ellipsis `: the challenges and negotiations of social and mobile media privacy for non-dominant youth. *INFORMATION COMMUNICATION & SOCIETY*, *18*(3, SI), 281–294. http://doi.org/10.1080/1369118X.2014.989251

Xu, H., & Dinev, T. (2012). The security-liberty balance: individuals' attitudes towards internet government surveillance. *Electronic Government, an International Journal*, *9*(1), 46. http://doi.org/10.1504/EG.2012.044778