Digitalization and Privacy

A systematic literature review

Svensson, Måns; Rosengren, Calle; Åström, Fredrik

2016

Document Version:
Publisher's PDF, also known as Version of record

LUND UNIVERSITY

DIGITALIZATION AND PRIVACY

A SYSTEMATIC LITERATURE REVIEW

Måns Svensson, Calle Rosengren and Fredrik Åström

Published by LUii 2016

Digitalization and Privacy

A systematic literature review

Måns Svensson, Calle Rosengren and Fredrik Åström

LUND
UNIVERSITY

Digitalization and Privacy

A systematic literature review

Lund University Internet Institute, Lund University Sociology of Law Department and Lund University Library.

Research coordinator:
Måns Svensson, Assoc. Professor of Sociology of Law

Authors:
Måns Svensson
Calle Rosengren
Fredrik Åström

Report nr 4 published at LUii

ISBN 978-91-982312-4-3
ISBN 978-91-982312-5-0 (PDF)

Cover image: Peter Frodin
Graphic design and Copy-editing: Peter Frodin

Printed in Sweden by Media-Tryck, Lund University, Lund 2016

Abstract

The research area of *Digitalization and Privacy*, as defined and delimited within the context of this literature review, (mainly through the selection of search strings), is in a phase of development. The present study has been delimited to articles in English that have been published in scientific peer-reviewed journals. During the past ten years, the number of scientific articles per year has increased more than five times. For example, a search of the database WEB OF SCIENCE for the year 2006 renders 13 matches, while an identical search for the year 2014 renders 72 matches.

In the present systematic literature review, two types of investigations have been conducted. First, a bibliometric analysis that aims to produce a comprehensive overview of the current state of the research in the area at a statistically analytical level. Second, a systematic literature study that has identified relevant scientific articles, analyzed their content and categorized them.

The bibliometric analysis demonstrates that research on digitalization and privacy is quite strictly divided, mainly between three scientific fields. In other words, communication between the various fields (i.e., intertextual references and citations of each field's research) is somewhat limited. The research fields can be described as: (a) a technical field that is largely concerned with systems development, (b) a legal field that focuses on issues regarding legislated protection of privacy, and (c) a social sciences and behavioral sciences oriented area that includes informatics, psychology, sociology, political science and marketing and management research and more.

This systematic literature review, based on close reading of all included articles, shows a lack of clear, mutually shared, conceptual terminology and common understandings of methodologies within the various scientific disciplines. However, there are a number of areas (or focuses of research) that recur frequently. The five dominant areas are: (a) technology, (b) legislation, (c) the state, (d) theory, and (e) working life.

Further, the research identifies different approaches to digitalization and privacy. First, as a problem (or, perhaps, a challenge) that can be managed using new, improved and more privacy-sensitive technology. Secondly, as an opportunity to work towards achieving good values such as improved health, through practical applications of potentially sensitive data. Thirdly, as a threat to citizens and employees. And, finally, as a relationship of exchange between usefulness and risks, for example, with regards to state needs for information in order to prevent threats and protect the citizens rights of privacy.

It is also strikingly clear that there is insufficient knowledge of the relationship between digital surveillance and potential behavioral changes in society. Various studies highlight that a lack of respect for privacy risks leading to reduced Internet use and reduced political involvement (at least on the Internet). However, at this point in time there is no empirical evidence to support that this is the case.

Content

1. Introduction

The present literature review has been conducted by Lund University (as regulated in the agreement of 2015-04-23) and commissioned by The Swedish Privacy Committee (Ju 2014:09). The Swedish Privacy Committee's task is declared in Directive 2014:65 which states that the parliamentary joint committee shall: "From an individual perspective, map and analyze the actual and potential risks concerning privacy issues that may occur in the use of information technology, both in private as well as public contexts; further, within the context of this commission, it shall monitor the effects of the legislation process of 2011 to improve constitutional protection of privacy, as well as take into consideration general social and technological advancements, and based in the conclusions of the mapping and analysis, follow up on the deliberations concerning Protection of Privacy SOU (2008:3) and particularly determine, with regards to the establishment of a committee for the protection of privacy, whether the mission for the committee could suitably be carried out by an already existing authority, as well as propose necessary constitutional amendments. "

The mission as stated by the Swedish Privacy Committee that this literature review is based on has been specified as follows: The literature review shall present relevant research of interest that has been conducted both in Sweden and abroad concerning its impact on individuals, groups and societies when surveilled, or believe they are being surveilled, or could become the object of surveillance (even if they are not). This also applies to studies on the impact on people, including organizations and corporations, through new possibilities to actively surveil/control others. Impact refers to how peoples attitudes/perspectives and behaviors have changed. The literature review shall also examine whether studies have been conducted within specific areas, such as patients' attitudes and how they may have been impacted, or whether there has been an impact on employers' behaviors in conjunction with recruitment of new staff, as well as toward their present employees. If potential differences in perspective and behavior according to gender have been studied, this shall be highlighted, as should differences between age groups. For example, studies on children who have grown up in a digital environment are of interest.

The methodology used for this project consists of a scientific, systematic literature review as well as bibliographic analyses. Searches in Swedish produce very few matches, and therefore, that part of the project has been postponed. The focus is therefore on peer-reviewed articles in English.

2. Methodology

Fundamentally, the systematic literature review constitutes a form of research that collects, analyses and summarizes studies within a specific field (or based in a specific question). Therefore, the systematic literature review can be described as an effort to summarize the state of knowledge within a certain area through the structured and systematic gathering and close reading of scientific studies. The collecting of various studies is generally carried out through searches for scientific publications in databases (e.g.. EBSCO or Web of Science) and is therefore informed through relevant key words. By ensuring visibility of the method, its point of departure and the criteria used for the searches, transparency is ensured, and the possibilities of repeating the study are increased. Three steps have been followed in the development of the present literature review, as described by Tranfield (2003) et al. in Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review (2003): (a) the planning stage; (b) to search, identify and organize the publications, and (c) extract and evaluate. At each step, there are a number of deliberations to consider with regards to both search criteria and which publications to include or exclude. The process of applying Transfield's (et al.) method in the present study is detailed below.

(a) Planning the study

The literature review focuses on issues related to digitalization and privacy. Surveillance in digital medias, as well as the potential impact on attitude, behavior and privacy are of particular interest. If possible, the study shall highlight the options available for specific groups (based, for example, in age and gender), as well as identify thematic areas that are of interest and relevance to the research question.

There are significant restrictions to the present study, due to the need to restrict the systematic search for scientific publications to scientific articles written in English. Publications in this area written in Swedish are generally not scientific, meaning that they have not been peer-reviewed and have therefore not been submitted to a process that guarantees scientific rigor. This particularly applies to articles, but also to a large extent to books and reports. PhD dissertations are a significant exception that conform to scientific rigor, but nevertheless do not meet the requirements of the present study. Having said that, it is important to emphasize that relevant information on specifically Swedish conditions may be present in the so-called gray literature (reports, governmental publications, specialized books etc. that have not been peer-reviewed), but has not been reviewed here.

(b) Search, identify and organize articles

From a privacy perspective, the digitalization of society has brought great challenges which pertain to several different research fields. The issues covered concern the relationships between state and citizen, consumer and corporation, employer and employee, as well as between individuals. Technology offers new methods of communication and services to consumers and citizens, but also entails, as yet, unrecognized possibilities to map individual opinions and behaviors. The ambition of the present literature review is to paint as broad a picture as possible of the state of the research concerning digitalization, privacy and the ensuing effects on people.

Two databases were deemed particularly appropriate for this systematic literature review, namely SCOPUS and Web of Science (Core Collection). SCOPUS, owned by Elsevier, indexes roughly 22,000 scientific articles and has a broad coverage of different disciplines and topics. Web of Science is a database (which, e.g. , includes 12,000 scientific articles of the highest scientific rigor) published by Thompson Reuters, and indexes international research literature, mainly journal articles written in English. The advantage of using this database is the rich information content it includes which allows for detailed bibliometric analyses.

(c) Extract and evaluate the materials

In order to provide as comprehensive a summary of the state of the knowledge as possible, in the present review we have selected to conduct both a bibliometric as well as a systematic literature review. Fundamentally, a bibliometric analysis is concerned with summarizing the research fields that are conducting research on certain phenomena, as well as the extent to which these fields relate their findings to other fields also studying the same phenomenon, using statistical analyses of texts and the characteristics of various text collections. A systematic literature review, then, is fundamentally a summary of relevant literature within a given area. The collecting of materials is based in careful and systematic methods of literature searches. Contrary to, and complimentary to, the bibliometric analysis, this method also includes a qualitative component since the literature retrieved from the searches is also read and evaluated.

3. Conclusions

Bibliometric analysis

In order to provide a comprehensive overview of the research fields that focus on issues concerning privacy in digital contexts, as well as which issues are being researched, bibliometric analyses of the research literature have been implemented.

The bibliometric analyses are based in the Web of Science (WoS) databases, which are a collection of databases that primarily index articles in English published in international science journals. The disadvantage of using this database is that research literature published in other languages and/or other types of documentation (f.ex. books) are not included. The advantage is that WoS, aside from using common forms of meta-data, also indexes the references included in the scientific texts, which makes it possible to conduct different types of citation and terminology analyses.

To identify the research literature included in WoS that addresses issues concerning privacy and surveillance, the following search strings were used in the topic field (which covers concepts and terminology that appear in the titles, abstracts and keywords): (Surveill*) AND (online* OR digital* OR Internet*) AND (behav* OR attitud* OR privac* OR "norms"). Searches were further delimited to the time period 2005-2015, and according to document type, where only original and general overview articles were included in the searches (figure 1).

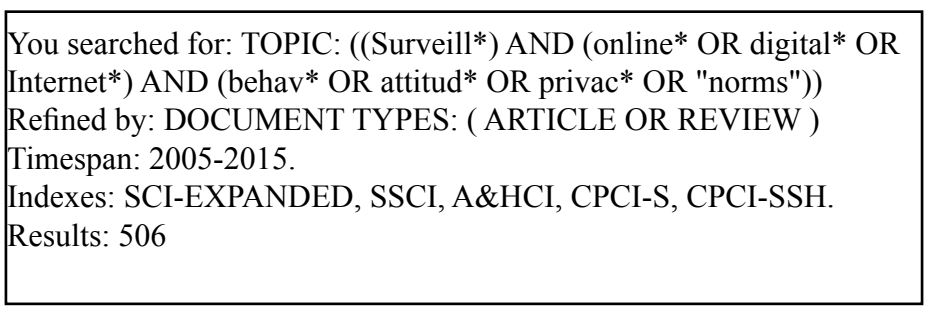

Figure 1. Search string for the Web of Science searches that the data collection for the bibliometric analyses were based in.

The search resulted in 506 articles; however, concepts such as "surveillance", although they may be contextual to digital contexts or issues concerning behavior, may also

retrieve scientific articles which are not relevant to the context analyzed here. An example of this is "surveillance", which is an important concept in epidemiology when surveilling patients in conjunction with operations, or, for example, health issues and risk behaviors among substance abusers. In other words, this refers to surveillance as a health care matter in conjunction with the management of patient information, rather than security and privacy issues. In order to avoid irrelevant literature as far as possible, searches were further delimited by excluding roughly 50 WoS categories (categories that mainly describe the primary content of the indexed journals), which resulted in a new set which included 311 articles (Figure 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 HEREDI-TY OR ENDOCRINOLOGY METABOLISM OR FOOD SCIENCE TECHNOLOGY OR DER-MATOLOGY OR ONCOLOGY OR VETERINARY SCIENCES OR IMMUNOLOGY OR TOXI-COLOGY OR ENGINEERING BIOMEDICAL OR SURGERY OR CLINICAL NEUROLOGY OR PEDIATRICS OR BIODIVERSITY CONSERVATION OR PATHOLOGY OR BIOCHEMIS-TRY MOLECULAR BIOLOGY OR SUBSTANCE ABUSE OR OBSTETRICS GYNECOLOGY OR MEDICINE RESEARCH EXPERIMENTAL OR AGRICULTURE MULTIDISCIPLINARY OR ERGONOMICS OR REHABILITATION OR ZOOLOGY OR VIROLOGY OR GASTROEN-TEROLOGY HEPATOLOGY OR UROLOGY NEPHROLOGY OR OPHTHALMOLOGY OR OCEANOGRAPHY OR NUCLEAR SCIENCE TECHNOLOGY OR METEOROLOGY ATMOS-PHERIC SCIENCES OR ENVIRONMENTAL SCIENCES OR MARINE FRESHWATER BIOL-OGY OR LIMNOLOGY OR MATHEMATICAL COMPUTATIONAL BIOLOGY OR FISHER-IES OR ENTOMOLOGY OR EMERGENCY MEDICINE OR ELECTROCHEMISTRY OR CHEMISTRY ANALYTICAL OR CARDIAC CARDIOVASCULAR SYSTEMS OR BIOCHEM-ICAL RESEARCH METHODS)
Results: 311

Figure 2. Research areas excluded from the Web of Science search.

This restriction resulted in a limited amount of documents that included fewer irrelevant documents. However, when counting the individual articles that were retrieved, it becomes clear that a number of articles remain which lie beyond the focus of this literature review (exemplified below by the last 10 documents retrieved from the search). Further delimitations of the searches in WoS are difficult to conduct since there is a risk of excluding too much potentially relevant literature.

Brown, S. 2015) Moving elite athletes forward: examining the status of secondary school elite athlete programs 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.

Figure 3. Examples of heterogeneity in the articles retrieved from the Web of Science search. The ten, latest indexed articles in the document set.

WoS data on the remaining 311 articles was downloaded. Bibexcel was used to process the data (https://bibliometrie.univie.ac.at/bibexcel/), which is a program used for bibliometric analyses that allows information from WoS to be refined in order to analyze specific fields, for example, titles, authors or cited references; but also sections of specific fields, for example, the titles of journals of cited references. The data retrieved

through Bibexcel was then fed into VOSviewer, version 1.6, (http://www.vosviewer.com/), which is a program used to process and visualize bibliometric network analyses.

Analysis of research fields

In order to identify the research fields that study issues pertaining to surveillance and privacy, the journals were analyzed for co-citations. The objective here was to study the literature used in the research by analyzing the reference lists and presume that articles, or in this case journals, that are co-cited are topically related. When hundreds or thousands of articles that include tens or hundreds of thousands of references are analyzed using this method, co-cited articles or journals will then form clusters that represent different research orientations or research fields.

The following analysis is therefore based in how often cited journals appear together in the reference lists for articles identified in the search for literature on privacy and digital surveillance. The map is based on analyses of the 500 most frequently cited journals. The map shows often cited journals - represented by the size of the nodes and journal titles - and how the journals are positioned in relation to each other, based on how often they are co-cited. When frequently co-cited, they are positioned closer to each other, and when co-cited less frequently, they are positioned further apart. Apart from co-occurrences represented by closeness of proximity, a cluster analysis to identify statistical relations also based in co-occurrences has also been implemented. The clusters are represented by different colors. The analysis is further complemented by connecting lines that represent stronger relations (more than 1,000 co-citation links), which visualize the extent to which the various clusters are linked, and, by extension, to what extent the different research fields communicate with each other (see below).

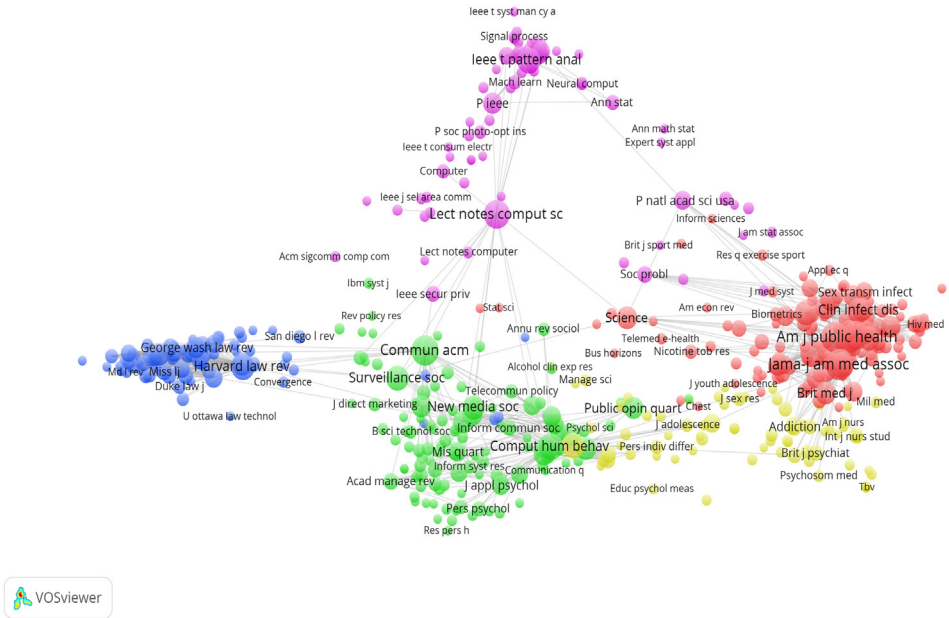

Figure 4. Co-cited journals.

On the right side of the map we find two clusters that mainly contain medically oriented research (together with clinically oriented psychology and psychiatry), despite attempts to delimit the search, that largely concern epidemiological research and research on illnesses and risk related behaviors (ranging from diabetes to sexually transmitted diseases and addiction oriented research); but also medical and behavioral science research that matches the criteria for relevant material in the present study. On the left side of the map we find a cluster that represents legal research. In the upper middle section of the map we find computer science research which deals largely with the development of systems and networks, and various methods of signal processing and pattern analysis, rather than the effects of surveillance of individuals and issues concerning privacy etc. (see below).

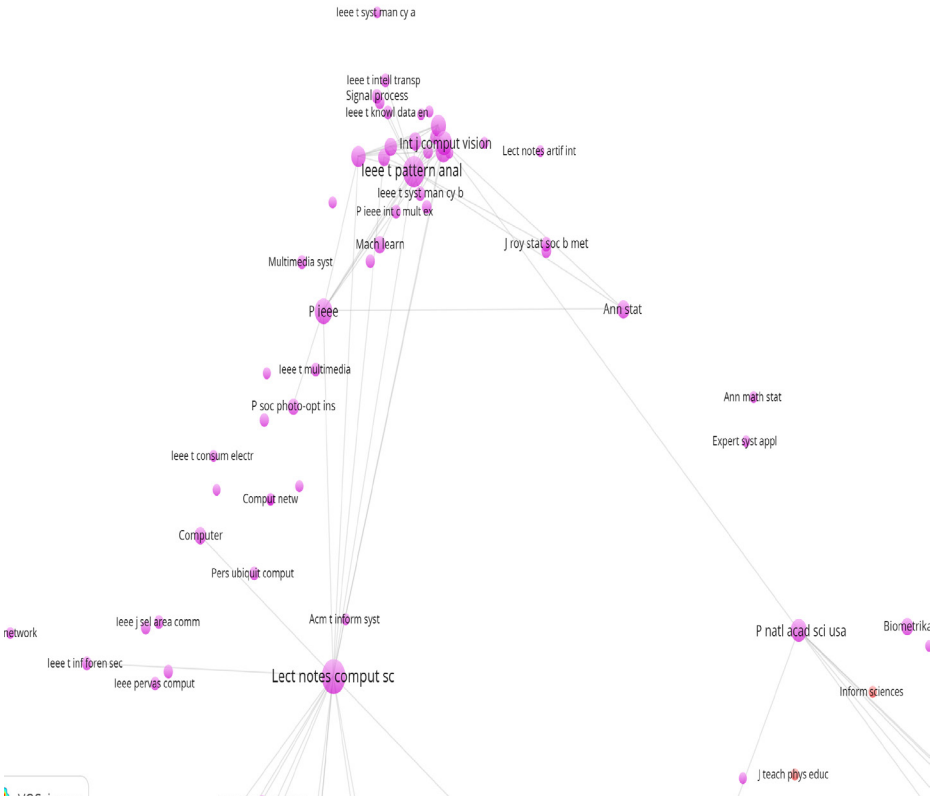

Figure 5. Magnification of the map of co-cited journals: computer science clusters.

The cluster of most interest, from the perspective of the present study's theme, is found in the lower middle section of the map (see below). Research represented by journals in the fields of informatics, psychology, management and marketing research, sociology and other social sciences, including library science and information science, and media and communications science are accumulated here.

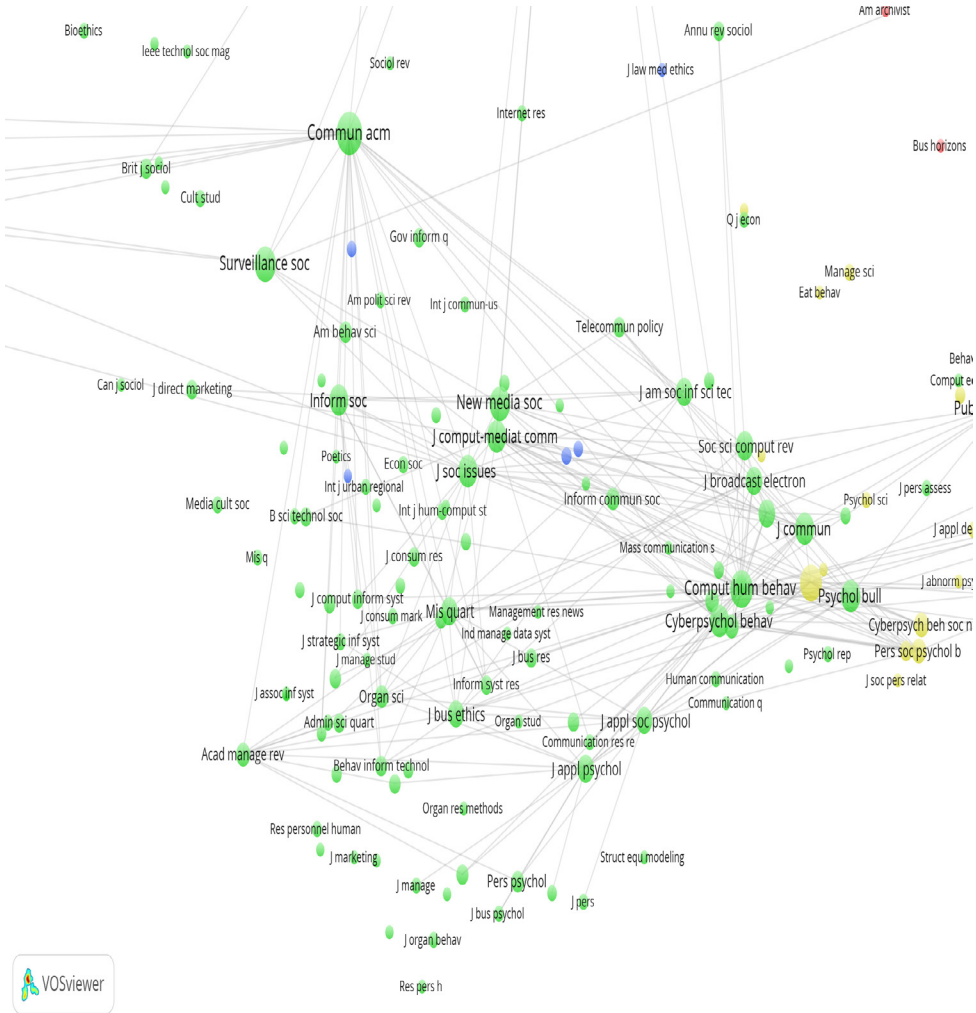

Figure 6. Magnification of the map of co-cited journals: social sciences cluster.

In other words, we see a rather strict division in the research on privacy and surveillance, and that three predominant focuses emerge: a technological perspective which is largely concerned with systems development, a legal perspective with a focus on issues surrounding legislated protection of privacy, and a more social sciences oriented perspective, which among other things includes informatics, psychology and marketing and management research. There are few links between the various main clusters. One might expect stronger links between computer science research on systems development and the more user-orientated field of informatics (largely human-computer interface research), but that is not the case. The strongest links between the research fields are found within the more social sciences related cluster where informatics, psychology,

sociology, political science and marketing and management research appear to mesh across disciplinary borders.

Analysis of terminology

To move forward and identify not only which research fields conduct research on privacy and surveillance issues, but also which topics are objects of research, an equivalent analysis was carried out, which - in contrast to the analysis of research fields - was not based in co-occurrences of reference lists, but rather in co-occurrences of concepts and terminology. Titles of articles, abstracts and key words that describe the content of the articles were retrieved from the articles identified in the WoS search. Similarly to the previous analysis, co-occurring concepts in the documents were grouped together.

In other words, the map illustrates the relationship between the 1,465 terms that emerge at least twice; those that often appear together are positioned closer to each other on the map, while terms that co-occur less frequently are positioned further apart. The map also indicates that larger amounts of terminology with stronger links are to be found in the red zone, while areas with fewer terms and weaker relations progress increasingly toward green and, finally, toward blue.

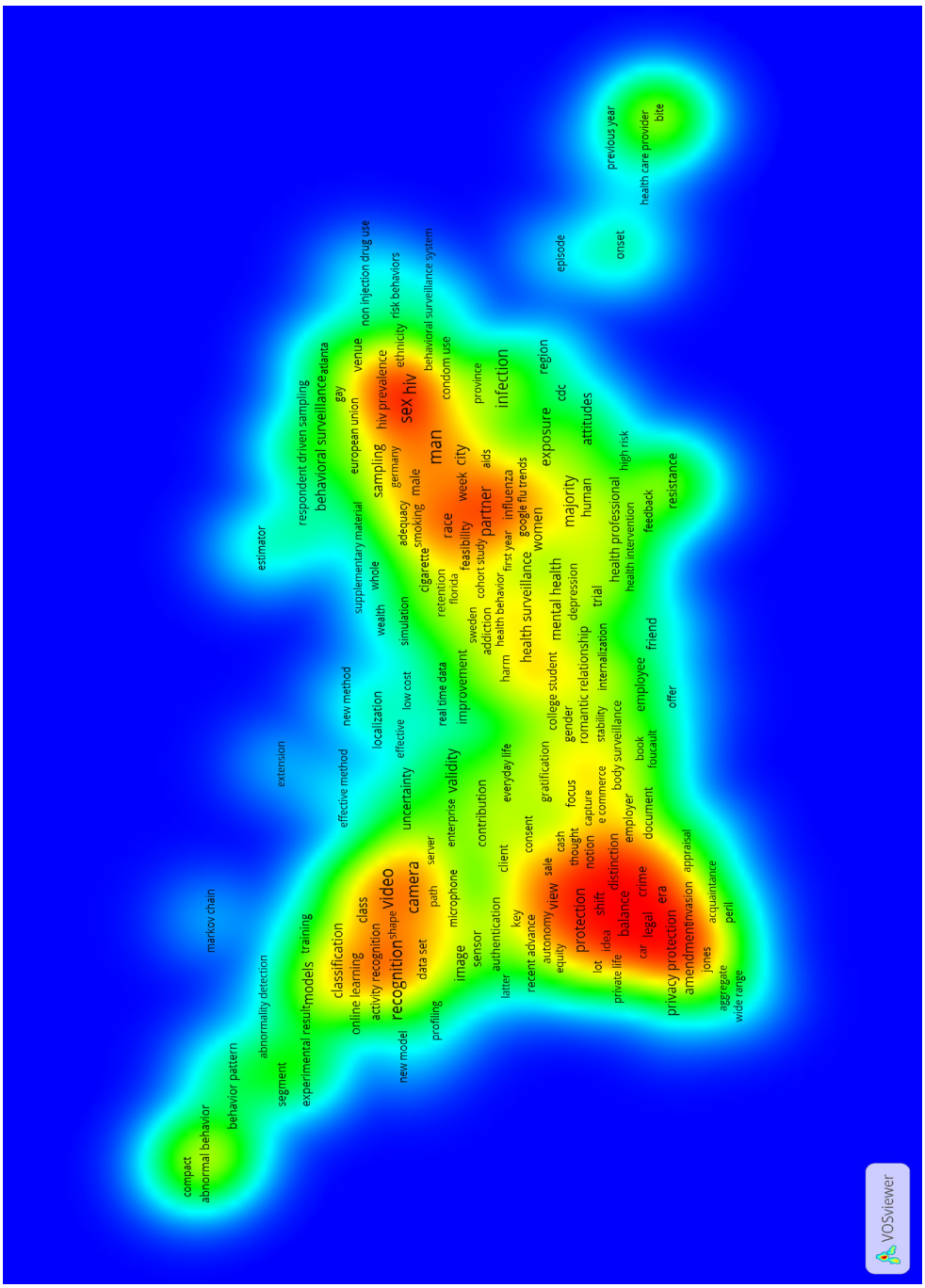

Figure 7. Co-occurrences of terminology in titles, abstracts and key words.

Three main clusters of terminology emerge in the map (figure 7). On the right, we find terminology related to medical research, where surveillance is mainly seen as an aspect of health care efforts to prevent the spread of epidemics and to follow health developments, rather than the control of people.

On the upper left side of the map there is a cluster that corresponds with the research on technological science previously identified in our analysis of the research fields (figure 8). Based on the terminology in this cluster, it is clear that this research is largely concerned with the development of systems and technologies for surveillance and recognition of data patterns.

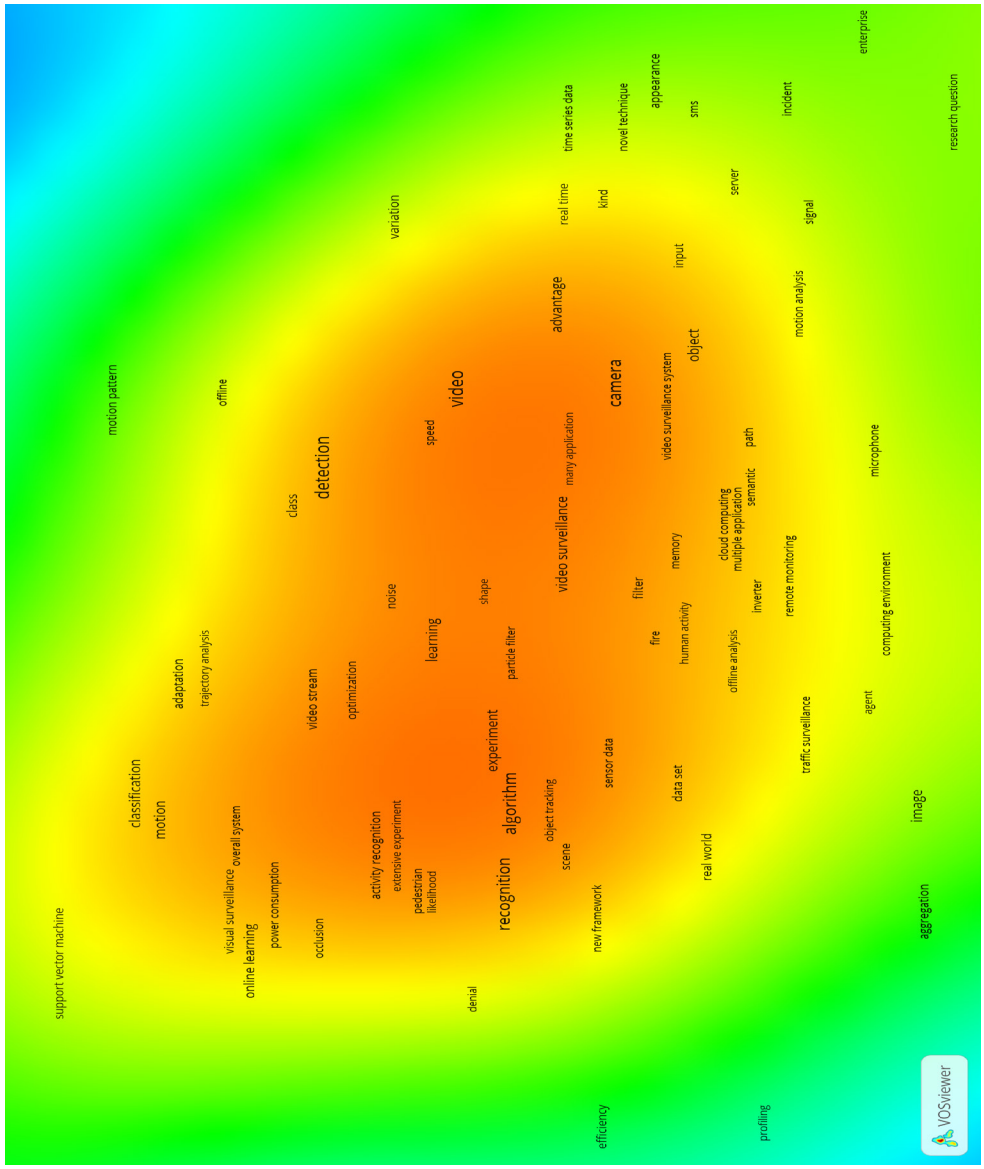

Figure 8. Magnification of the map with co-occurring concepts: computer science clusters.

On the bottom left side of the map, we find a cluster that appears to gather the legal and social sciences and behavioral science research fields from the map of research fields. These concepts relate to legal, political, and social issues such as protection of privacy, legislation and the links to constitutional law, legitimacy and behavioral and social norms (Figure 9).

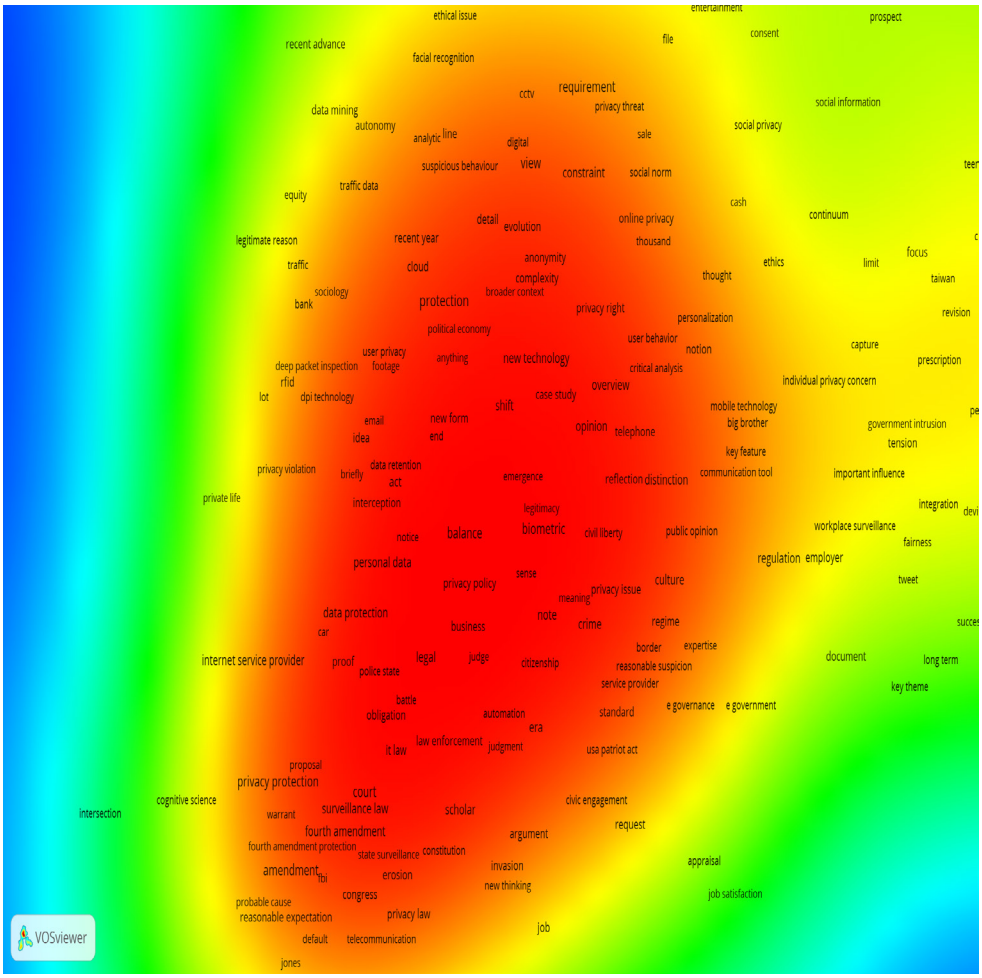

Figure 9. Magnification of the map with co-occurring concepts: Social science and legal clusters.

Similarly to the map of research fields, we find few links between the social scientific aspects and technological or medical aspects, while we also find that both social scientific and legal research have accumulated here according to terminology within the same cluster. However, this should probably be viewed as an indication that these research fields largely use the same, relatively general, terminology, rather than this being a case of two research fields communicating with each other.

Systematic literature review

This literature review has focused exclusively on peer-reviewed scientific articles published in English between 2005 and 2015. Peer-review requires that the articles have been reviewed by external and impartial expert researchers whose mission is to ensure that the articles and studies meet all the requirements for scientific rigor. The search method used here is a so-called boolean search (AND/OR/NOT). The two databases used (SCOPUS and Web of science) have slightly different functions and therefore these searches will be presented separately. The interface allows for searches within either/and/or abstract (AB), and subject area (SU). Conducting a search using key words makes it possible to retrieve texts in which the authors themselves have specified a number of keywords. Searches for these types of subject words are particularly well suited to areas that already have well established terminology and a mutually shared definition of the various concepts. Alternatively, a search of the abstracts can be also be conducted. This allows for the possibility to search a somewhat broader field, where different terminology may be used to describe roughly the same concepts. Additionally, a broader search generates a larger amount of material which therefore needs to be restricted in the next step.

SCOPUS

Search terms and their internal relationships are linked to the discussions concerning the mission of this study, as described in the introduction. The literature search has focused exclusively on peer-reviewed scientific articles published in English between 2005 and 2015. Using the following key words: surveillance, internet, online, digital, behavior, attitudes and privacy, this search string was generated:

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”**))

The search generated 342 articles for the following years of publication:

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

The search results read as follows, based in the countries of publication (this does not provide information about where the research was conducted, since researchers publish material in international journals):

Country of publication	Number
USA	139
Great Britain	43
Australia	21
China	21
Canada	19
Italy	11
South Korea	10
The Netherlands	9
Taiwan	9
Germany	9

Web of Science (core collection)
Searches were conducted using the "Topic" function in this database, and included searches for "Titles", "Subject Words" and "Abstracts." Using the following key words: surveillance, Internet, online, digital, behavior, attitudes and privacy, the following search string was generated:

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

Refined by: DOCUMENT TYPES: (ARTICLE OR REVIEW)

Following an initial review of the search results, it is apparent that many of the articles focus strictly on medical issues. For example:

Grigorescu, V. I., DAngelo, 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 Womens Health*, *23*(12), 989-994.

In order to exclude this type of medical articles, we used the function, "Web of Science Categories", which makes it possible to exclude a number of areas that were determined to be irrelevant to the research question. This provides a manageable quantity of articles that are relevant to this study's mission. We assess that the following categories can be excluded from the search:

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.

Following automatized exclusion there remained 330 articles spread over the following database-indexed areas:

Areas	Number
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

Country of publication	Number
USA	174
ENGLAND	40
AUSTRALIA	27
CANADA	17
ITALY	16
P.R. CHINA	12
NEW ZEALAND	8
TAIWAN	7
SOUTH KOREA	7
NETHERLANDS	7

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

Extraction and evaluation of the materials

The total number of 672 articles retrieved using the previously described criteria and databases were then imported and sorted using the reference management system Mendeley. The screening process is described below.

An initial screening focuses on removing duplicates. After removing the (147) duplicates, 525 articles remained. Articles not published in English (6) were then removed, leaving 519 articles. Based on the fact that titles were not deemed relevant to the subject, 70 articles were removed, leaving 449 articles after the initial screening. All 449 abstracts were then printed and submitted for close reading. A second screening was conducted to match the following categories:

Y (not relevant to the subject) = 260 articles were removed.
X (Not peer-reviewed scientific articles) = 17 articles were removed.

This left 172 articles for analysis. These articles were read and categorized based in research focus and object of study. The following areas were identified (number of articles indicated in brackets):

Technology (27)
Legislation (25)
State (23)
General theoretical arguments (21)
Work (12)
Knowledge and behavior among young people (17)
Health (14)
Commerce (12)
Private relations (9)
Human rights in digital environments (4)
Sousveillance (3)
Other (5)

A list of the fields follows below.

Technology

27 articles

In general, the articles that describe the technological aspects of Internet surveillance are overwhelmingly development and solution oriented. I.e., they focus on how to develop the Internet toward improved user-friendliness and protection of privacy using technological solutions. Concepts that are used to describe how privacy protection can be "built in" to technology fall under "Trusted Computing" (Shiguo et al. 2009; Winkler och Renner 2011), "Privacy Aware Design" (Wicker 2011) and "Privacy by Design" (Cavoukian et al. 2012). There are a few articles (McKee 2011; Mitchelfelder 2009 and Vitaliev 2007) that adopt a more critical perspective and highlight the threat that technology poses to privacy and the right to private life. In order to increase awareness and to address issues concerning privacy on the Internet, the following appeal was formulated by McKee (2011, p. 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."
In relation to this development in technology that increasingly threatens private life, Wicker and Schrader also appeal to all engineers to combat this development: "Engineers and computer scientists thus have a moral obligation to avoid design choices that are unnecessarily privacy invasive." The principles that should guide the design of the technological aspects of the future Internet are termed "Privacy-Aware Design Principles" which include five points that are intended to increase both transparency of the collected data as well as the possibilities to influence the type of information collected:

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

Similarly, Winkler and Renner (2011) discuss how privacy can be protected in terms of "trusted computing." More specifically, the article focuses on video surveillance of public spaces for crime prevention purposes, as well as various technologies for storing and processing potentially sensitive information generated by surveillance. Within this

context, it is worth pointing out that the boundary between video surveillance and surveillance in digital environments is becoming increasingly blurred, and the technologies are merging. The article discusses a number of different approaches, for example, separating generated data that relates to private information from information on behavioral data. "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." Alternatively, image information that could disclose an individuals identity should be removed by using a so-called "respectful camera" which "detects and blanks peoples faces in captured images." The encryption tool "PICO" is mentioned here, which can be used to encrypt sensitive information of a private nature, and where decryption of collected material is only possible after a crime has been committed (Winkler and Renner 2011, p. 17). Babaguchi and Nakashima (2015) focus on the issue of how to manage potentially sensitive information collected through video surveillance. Their article focuses on a number of specific projects (PriSurv, Digital Diorama (DD), and Mobile Privacy Protection (MPP)) that all aim to strengthen people's right to private life. Another concept that emerges in this context is "Privacy by Design" (PbD), where issues of privacy are "embedded as a core functionality in the biometric system" (Cavoukian et al., 2012). The authors argue that issues concerning privacy should be the starting point when developing new technology and new business models, rather than be approached in the final stages, or not at all.

PbD is also mentioned by Shilton (2012) who first and foremost focuses on privacy issues related to user-generated data. The article describes a development where people using apps and wearables measure and communicate on topics such as exercise regimes, and eating and sleeping habits in social networks. Here, PbD could lead to a more focused approach to how to manage potentially sensitive information during the development phase of these types of products and services; for example, by clearly stating the type of information collected, but also by making it easier for the user to manage the settings for how information is collected as well as communicated.
Shiguo et al. (2009) describe the latest technology developments within multimedia as well as user information that is stored in connection with certain online TV services. Various solutions for protecting and managing sensitive information using, for example, different forms of encryption systems are also discussed.

Estee (2015) describes the development of different technologies to track user behavior on the Internet within a historical context from the 1990s up until now, with a particular focus on "cookies" (web based files containing user information stored on the user's computer), the development of these technologies in various forms as well as the development of other related techniques to protect the user's identity. The article highlights the need to inform and educate young people and students of this technology. The final chapter "Taking Back Our Digital Identities" states: "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, p. 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., DOrazio, 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

Legislation

25 articles

Overall, practically all the articles focus on law's inability to protect the individual's rights as a result of the rapid emergence of digital technology. A key issue in the articles concerning USA-specific conditions with regards to legal aspects of digital technology and threats to personal privacy is the "Fourth Amendment" (Desai 2014; Hu 2013; Kerr 2010; Solove 2005), which constitutes an important cornerstone of the American Constitution. The section of the Fourth Amendment debated here concerns the individual's right to private life. The starting point for all the articles is the assumption that digital developments have led to a situation where law no longer adequately protects the individual's right to privacy.

Kerr (2010) seeks to apply the Constitution and the Fourth Amendment to an Internet-related context and takes his starting point in the confusion that surrounds the types of digital communication that are protected by law (f.ex. e-mail and text messages). The ambition is to attempt to create a system that provides as strong protection in the digital world as in the physical. More specifically, the distinction between the terms "inside" and "outside" used in a police report are discussed. The terms describe individuals' expectations on their private life, and the right of the police to observe and collect information on individual behavior in the context of the physical environment the individual is situated in. The law distinguishes between the right to private life depending on whether you are in a public space or your own home. The issue debated in the article, therefore, is how to translate this distinction to a digital context.

Desai (2014) also discusses the individual's right to private life in relation to police investigations, but rather in terms of "forward looking" and "backward looking" surveillance methods. Forward looking surveillance describes the type of surveillance that follows when a judge grants a special permit and includes, for example, GPS-monitoring and phone tapping. In order to be granted such a permit, there must be a suspicion of some form of criminal act. The permit also describes the type of information that may be collected, as well as the purpose for which it may be used. The problem discussed in the article is backward looking surveillance, which is described as follows: "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, p. 582-583). Above all, this describes a reasonably simple method to create a detailed description of an individual's life, which can be a threat to political organization and expression.

Another key theme in the articles that focus on legislation is the right to information (Cover 2015; Grodzinsky and Tavani 2005; Konstadinides 2011; Mantalero 2014; Peppet 2014; Roberts 2015). This takes its starting point in the confusion surrounding who owns the information generated by users on the Internet as well as who owns the rights to the data, and for what purposes they may be used. Mantelero (2014, p. 644) describes the problem in the following manner: "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 users' self-determination." The legislation intended to protect the individual's right to privacy is based on the principle of "Notice and Consent"; i.e, the user shall have the right to be informed of the collected data and also have the option to consent or deny consent. Mantelero (2014, p. 652) describes the problem of Notice and Consent: "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." In other words, trading in data has led to data being used in new contexts that were not originally intended. This, combined with the fact that data from other contexts can also be combined and analyzed, means that patterns in both individuals and groups can be revealed. Peppet (2014) addresses the emergence of the "Internet of Things", as well as potential problems concerning how data is stored and used in this context. The Internet of Things is a collective term for computer-based technology that is built in to (often mobile) products that register daily activities such as exercise, eating and sleeping habits. It is in this context that the author poses the question, "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, p. 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 Kerrs 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

The State

23 articles

Articles that focus on the relationship between the state and its citizens in a digital context share in common questions concerning how, and in which contexts, it can be deemed legitimate for the state to actively collect information on individuals' online communication, as well as the potential implications of a lack of trust or political involvement in situations when the surveillance is experienced as unmotivated or overly intrusive. However, not all research results are in agreement; rather, they require taking into consideration individual countries' unique characteristics as well as the interaction between the experienced usefulness of the surveillance, age, education, occupation and political opinions.

In the case of China, where the totalitarian one-party state is in itself illegitimate, viewed from a strictly democratic perspective, the discussion revolves around the issue of surveillance as a pure instrument of power to reinforce the state's position vis-à-vis its citizens (Jiang and Okamoto 2014; Wang and Hong 2010). One of the articles (Jiang and Okamoto 2014) states that 42 per cent of Chinas total population of 1.3 billion citizens are Internet users. Web searches using various search engines are one of the most common activities among these 591 million Internet users. Jiang and Okamoto's (2014) article focuses on the state owned search engine Jike, which the authors describe as an attempt by the Chinese communist party KKP "to control information, enhance legitimacy and achieve cyber power through both technological regulation and creation" (p. 100). According to the authors, "cyber power" is achieved by (1) reinforcing national identity and solidarity through the search engine's nationalistic interface, (2) the search results that are made available, and (3) its potential to spy on online user behavior. The first two points are described in some detail in the article, while the issue of how user information from the search engine is stored and used is discussed at a more hypothetical level. The authors explain that this is because the type of information being stored, and how it is used, is unknown.

Wang and Hong's (2010) focus on the Chinese blog sphere questions whether such a forum could potentially contribute to increased openness in China. The authors challenge the image of blogs and bloggers as social changers and argue that the Chinese state has successfully limited freedom of expression of this medium. "The expansion of Chinas use of cyberspace is matched by the governments 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 Chinas Bloggers are empowered by this new communication vehicle, which allows them to express themselves freely and deliberately, Chinas blogosphere is not leading to the overthrow of the dictatorship" (p. 76).

The articles that discuss the situation in China are highly critical of the country's regime, and there is an underlying assumption that Internet surveillance of its citizens has mainly contributed to reinforcing KKP's power rather than protect its citizens from external threats.

The issue concerning external threats, as well as the state's options to prevent them through Internet surveillance, is also a salient theme in the research and articles that focus on the American citizen-state. Redick et al. (2015) take their starting point in the debate that arose following the mass-surveillance program conducted by the National Security Agency (NSA), which to a large extent was carried out without the citizens' knowledge. An underlying presumption in this article is that surveillance in itself is legitimate and aims to improve the state's capacity to function: "Public sector organizations are increasingly using data to improve their performance, provide greater citizen engagement, and cultivate levels of collaboration and transparency" (p. 129). In other words, the starting point, here, is that far reaching surveillance of the citizens was (and is) legitimate, and that the challenge, instead, is how to better communicate the functions of these surveillance programs: "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" (p. 138).

It follows, then, that attitudes toward surveillance are influenced by how legitimate they are experienced as being. Legitimacy, in turn, is related to assumed/experienced threat assessments, as well as the state's capacity to prevent and counter such threats through surveillance. Dinev et al. (2008, p. 214) conclude that "The perceived need for government surveillance was negatively related to privacy concerns and positively related to willingness to disclose personal information." The notion that there is quite far-reaching acceptance for state surveillance in the USA is further confirmed by Dinev et al. (2006) who have conducted a comparative study of attitudes toward surveillance between Italy and the USA. The authors conclude that "Italians exhibit lower Internet privacy concerns than individuals in the U.S., lower perceived need for government surveillance, and higher concerns about government intrusion" (p.1). The article explains Italy's resistance to state surveillance partly due to a lower expectancy of risk, but also due to a lower degree of trust in the state.

Two studies on citizens' views on state Internet surveillance in the Balkans (Budak et al. 2013; Budak et al., 2015) highlight the importance of considering various demographic conditions in order to understand and explain different attitudes surrounding surveillance. Their analysis divides citizens into three groups: "(1) pro-surveillance oriented citizens, (2) citizens concerned about being surveilled and (3) citizens opting for better data protection" (p. 17). These groups differ according to age, education and occupation. For example, the statistical analysis shows that citizens with lower levels of education tend to be more pro-surveillance than those with higher education. Similarly, we see that people outside the employment market tend to be more pro-surveillance than employees. With regards to age, younger citizens are more pro-surveillance than

older. However, the younger group also expresses some concern for the risks involved with surveillance.

Cohrs et al. (2005) develop an understanding of how external threats influence attitudes surrounding surveillance. This position disagrees to some extent with the stances held by Redik et al. (2015) and Cohrs et al. (2005); instead, they argue that the assumption of threat does not necessarily influence attitudes surrounding surveillance.

Another key question of focus in the articles that discuss the relationship between state and citizen is whether the assumption of being surveilled when using the Internet has an impact on political involvement. Here, the conclusions are somewhat contradictory. Best and Krueger (2008) argue that fear of surveillance is a genuine threat to democracy since it has an impact on political involvement. "The findings suggest that the prospects of government 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 government monitoring and are more likely to perceive that the government 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 and Krueger 2008, p. 205).

However, there are studies that demonstrate, in part, opposing results. Kreuger (2005) shows that the largest spread of online political involvement also includes those groups that experience the threat of state surveillance as problematic: "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, p. 448).

The experienced threat of surveillance and lack of trust in the state's capacity to handle sensitive information about the citizens is also a key issue within the area of E-government. E-government is a collective term for the state's efforts to implement information and communication technology to simplify and improve societal services to citizens and corporations, as well as to make citizens' access to information easier, and to be able to actively participate in public governance. Fear of how the state uses personal and sensitive information generated by citizens on the Internet can impact trust between the parties and, in extension, the will to use various online services. Keymolen et al. state this argument (2012), however, it is not based in their own data; instead, they discuss this at a more theoretical level, as well as reviewing more tangible points that need to be considered in order to strengthen trust between the state and its citizens, and by extension increase voluntary use of digital services to share sensitive information online. Lips (2010) argues that there is significant acceptance to share sensitive information with the state, as long as it leads to improved societal services. In order for the exchange of information on citizens and societal functions to work smoothly, there

must be improved transparency of the information collected and how it is used. Haikola and Jonsson (2007) present a study on how the debate in the Swedish Parliament was formulated in the early days of the Internet, with regards to the relationship between the individual's right to privacy and the need for surveillance. They argue that even if voices against increased surveillance did exist, they were still in the minority compared to the prevailing discourse that was based in the assumption of an increased need to collect information on citizens.

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.issue15.49

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 2.0s 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 Chinas 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

General theoretical arguments

21 articles

The articles under this heading share in common that they do not primarily present their own empirical data; rather, they focus mainly on the overall theoretical discussions concerning the emergence of what is often referred to as "the surveillance society." Since the texts are mainly based on connected arguments that span across roughly 5 pages, it is difficult to briefly summarize the contents here. However, the Panopticon and Big Brother are two recurring concepts.

The great opportunities for key actors to follow individuals' behaviors using digital technology are described in several other articles with reference to the Panopticon (Farinosi 2014; Ganascia 2010; Grodzinsky and Tavani 2005; Humphreys 2006; Kandias et al. 2014; Jiang and Okamoto 2014; Russett 2011). Here, digital society is problematized based in the argument that it enables massive surveillance of all of society's citizens. But it also describes how digital structures can be used by everyone and thus strengthen the individual's power in relation to the powers that be.

Ego-Panopticism: this is described as increased opportunities for individuals to monitor and disseminate information regarding maladministration and abuse of power in society using digital media. In other words, a reverse Panopticon, or as they describe it, a "Counter-Panopticism." Panopticism refers, here, to Jeremy Bentham's model of the ideal prison, where the prisoner is always (at least potentially) monitored by the supervisor. "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, saknas sida).

Big Brother: Orwell's dystopian depiction of future surveillance society in the novel 1984 is frequently referenced (Giroux 2015; Kang et al. 2012; Mordini och Rebera 2012; Stančin and Tomažič 2010; Van Otterlo 2014; Vitaliev 2007). In Zuboff (2015), the term Big Brother is used to describe the downsides of the active commerce and accumulation of potentially sensitive personal information. Since the user data is collected in various contexts and then resold, it becomes unclear who has information about the user and the consequences this may entail. This is also described as "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, p. 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 technologys 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

Work

12 articles

On a general level, the articles show that monitoring employees' activities on the Internet is quite common. For example, Alder et al. (2008) report that as many as 63 per cent of US companies monitor their employees' Internet use. At the same time, a number of potentially harmful effects are highlighted, such as reduced trust in the employer, motivation and job satisfaction. However, the relationships are not immediately obvious; rather, whether surveillance has a negative effect on employees depends on how justified it is perceived to be, as well as a number of other factors such as length of employment, for example.

Ball (2010) situates the issues concerning employee surveillance in a historical perspective and argues that the phenomenon in itself is nothing new, but has, in fact, existed for a long time. However, digital technology has enabled more far-reaching and intrusive opportunities to follow the employees behaviors in detail. Furthermore, it is argued that this type of digital surveillance potentially has consequences for both employee health and well-being as well as motivation and creativity.

Alder et al. (2006; 2008) show that surveillance of employees' Internet use can impact trust in their employer negatively, which in turn also has consequences for job satisfaction, commitment and ambition to remain with the company - particularly when this takes place without prior consent or the aim having been clarified.

Samaranayake and Gamage (2012) also study employees' perceptions of, and attitudes towards, being monitored in the digital workplace. Their main conclusion is that the experience of being monitored affects job satisfaction negatively. "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 and Gamage 2012, p. 242).

However, a more in-depth analysis shows that this correlation diminishes the longer the employees have been employed. "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 and Gamage 2012, p. 243). However, it is also argued that negative experiences of surveillance can be prevented through information and clear policies. "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 and Gamage 2012 p. 243). This reasoning aligns well with Adler et al. (2006).

Wen and Gershuny (2005) discuss the legal aspects of digital surveillance of employees. Similarly to other articles that deal with the legal aspects of surveillance and privacy in a digital environment, they point out the difficulties that law has in keeping up with technological progress, which results in protection for the individual employee being weak. In situations where a case has reached court proceedings, the outcome has almost always been in the employers favor. "Court decisions have supported employer monitoring of employees email. Courts have even allowed the use of video cameras in employee changing rooms when the employers 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 and Gershuny 2005, p. 169). Finally, the article argues for the importance of companies to develop policies in this area. "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 and Gershuny 2005, p. 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., & ORourke, 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

Knowledge and behavior among young people

17 articles

This area of research deals with attitudes toward online privacy ("Privacy perception/ concerns"), primarily in relation to education. In this context, issues such as socio-economic class affiliation and differences in knowledge levels ("digital/privacy literacy") are also discussed, as well as various pedagogical approaches to improve individuals knowledge of the Internet and develop greater security awareness of how information is managed in digital environments. Or as Park (2013a, p.3) puts it: "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) points to large differences in levels of knowledge and understanding of privacy issues among Internet users which can be attributed to socio-economic status. There are appeals, in this context, for special measures to target vulnerable groups in order to even out class differences: "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 ones digital engagement"(Park 2013b, p. 698).

Oulasvirta et al. (2014) show that experienced privacy concerns in a digital environment increase when users are monitored/surveyed without the sender or the purpose being clear. The research project is described as follows: "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 collectors identity and intentions. Knowledge about intentions exhibited 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, p.1). Accordingly, transparency significantly reduces concerns. Based in this, the article concludes: "The present findings underline that both the data collectors 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 users' attention to the data collectors intention will have a stronger effect than would drawing attention to identity alone" (Oulasvirta et al. 2014, p. 5).

Berger et al. (2014) show that young people's experiences of being monitored on the Internet can lead to reduced Internet use: "The findings indicate a significant quantitative decrease in Internet activity of users believing to be monitored" (Berger et al. 2014).

Education in this area is termed "E-safety education" and is described as follows: "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, p. 240). The need for E-safety education targeted at young people is motivated by the particularly vulnerable position of this group, both as victims and culprits: "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 behavior, and can be responsible for harmful behavior to each other in the form of cyber-bullying" (Barnard-Wills 2012, p. 248). Steeves and Regan (2014, p. 299) describe a number of initiatives for Internet education programs targeted at young Internet users: "Educational programs typically reinforce this approach to privacy as informational control. For example, the European Unions Ins@fe initiative, the myprivacy.mychoice.mylife (2013) campaign created by the Privacy Commissioner of Canada (2008) and the US governments 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) refer to the tool "Gazela" which is intended to help young Spanish Internet users better evaluate and manage privacy issues 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 Sozialwissen-Schaftliche 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 Wont 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 dont 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

Health

14 articles

Much of the articles in this area concern the relationship between privacy issues and increased possibilities to follow Internet users' digital trails in order to predict and intervene in the spread of diseases. This can be done using, for example, the tool "Google trends." Nuti et al. (2014) describe this tool and its potential as follows: "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, p.1 ff). The study shows that Google trends compares in relation to other methods of estimating and mapping health and health behaviors. However, despite the tool's built in possibilities, it needs to be further developed: "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, p. 46). In relation to this, Gunn and Lester (2013) show that searches for suicide can be a good way to gain awareness of the problem at an early stage and implement interventions. Gu et al. (2014) also show that analyses of Internet searches can be an efficient way to quickly deploy responses to epidemics. Cooper et al. (2005) argue, however, that it is not only the spread of diseases themselves that generate searches on the Internet. In the article on cancer, they argue that media exposure of various medical conditions also tends to generate searches.

Common to the articles dealing with the possibilities, based on searches of individual digital footprints (Cooper et al. 2005; Gunn and Lester 2013; Nuti et al. 2014;), Blogs (Gu et al. 2014), twitter feeds (Velardi et al. 2014), Facebook likes (Gittelman et al. 2015) or their own programs that download information from various sources on the Internet (DAmbrosio et al. 2015) is that (surprisingly) they do not deal with privacy issues at all, but only see the opportunities of digital developments. The reason they appear in the search and screening process is that the term "Surveillance" is frequently used, but in those cases, to indicate that the collection of data can produce a good overview of a phenomenon.

The issue of privacy, however, emerges more saliently when the discussion relates to the digitization of regular health care services, for example, in discussions on electronic storage and management of sensitive personal information. For example, Kramer et al. argue (2012 , p. 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."

Within the area of E-health (M-Health or E-health), the management of potentially sensitive private information is also debated (Lupton 2012; Lupton 2015). Especially in relation to data generated by various health apps where the user voluntarily measures exercise habits and enters other types of health behaviors, such as diet. Lupton, in particular, discusses how the phenomenon (to be constantly measured and estimated) affects our self-image:

"Will the nagging voices of the health-promoting messages automatically issuing forth from a persons mobile device be eventually ignored by its user? Or will these messages incite even greater feelings of guilt and shame at ones 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 users sense of selfhood and embodiment? How will concepts of health itself be shaped and understood in a context in which ones biometric indicators may be constantly measured, analyzed 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, p. 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

DAmbrosio, 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

Commerce

12 articles

A key theme that emerges in the articles in the area of commerce is the study of the relationship between attitudes toward surveillance (privacy concerns) and consumer behavior (Park et al. 2012; Park 2014). The results of the various studies are somewhat contradictory. For example, Park et al. examine (2012) whether concerns that sensitive information could end up in the wrong hands impact consumer behavior on the Internet, and conclude that: "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 ones identity" (Park et al. 2012, p. 1023-1024). This would agree with Park (2014) who has studied how strong an impact a commercial web site that shows particular consideration in its management of private information has in relation to the number of users the site has.

Management of sensitive information refers, here, to whether the website user has the option to control the information he or she shares. "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 ones personal data and associated identities; widely regarded as one of the most vulnerable aspects of online use" (Park 2014, p. 360-361). As the following title suggests, A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites, it is doubtful that relying on commercial operators to increase their consideration for privacy through potential customers choosing not to use their services will have much impact. This is according to research that shows that the users' ability to impact the level of "information privacy" does not play a role in online consumer behavior. The research is described in the following way: "This article examines user control of privacy online as indicated by functional features of commercial websites. While prior studies have focused on whats 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, p. 360).

In contrast to the above, Markovic (2010) claims that issues concerning privacy and how personal information is managed do, in fact, impact consumer behavior, and that companies that do not pay attention to this fact risk losing customers. However, according to the author, the behaviors are not impacted as much by security settings on individual websites (as Park 2014 has researched, above) as by the organization behind the website.

In order to understand consumers' willingness or lack of to share personal information on the Internet, Li (2012) and Mekovic (2010) argue that we must take into account the perceived benefits of doing so in relation to the risks. In other words, in the final analysis, the decision is not only one of trust in the organization or an individual web site's design and functionality; rather, in order to understand consumers' online behavior the perceived benefits of sharing personal information must be taken into account. Li (2012) describes this calculation in terms of calculus (i.e., the trade-off between expected benefits and privacy risks).

Draper (2012) rejects the explanation that "consumer influence/power" is the focus of such data mining, since "consumer power" is equated with consumer benefit. Consumer benefit is described as follows: "…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, p. 403). Rather, it addresses the increased ability to produce targeted offers to consumers: "With the information these companies have about users, the ability to offer deals that are targeted based on an individuals online reputation or profile (accurate or not) is immense" (Draper 2012, p. 404), and concludes: "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, p. 405). What the companies describe as "consumer power" is, in fact, tailoring advertisements in order to maximize sales.

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

Private relations

9 articles

Digital technology has not only provided increased opportunities for companies and governments to monitor individuals. The same is also occurring in individual, private relationships. The focus here lies primarily on the possibilities for monitoring a partner's or former partner's activities on social medias. In other words, this does not concern any form of illegal activity, but, rather, the opportunity to follow another person's digital footprints on the Internet. Helsper and Whitty (2010) show that it is quite common to monitor (ex) partners' digital footprints, such as text messages, email and Internet history: "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 partners emails or read their partners SMS messages without them knowing and in a fifth of the couples at least one of the partners had checked their spouses browser history" (Helsper and Whitty 2010, p. 924).

Marshall (2012) has studied how ex-partners have managed their relationships on Facebook after breaking up, and the consequences this can have for health and wellbeing. The results suggest that those who maintain a friendship on Facebook after the relationship has ended may face obstacles in their personal maturity development and ability to move forward in life. However, somewhat surprisingly, this group expresses a number of positive aspects: "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, p. 523). This relates to Lukacs and Quan-Haase (2015) who further demonstrate that people who engage in intensive searches for ex-partners activities on Facebook generally experience a higher degree of emotional suffering.

Tong (2013) has also studied surveillance of ex-partners via Facebook, with a focus on the type of information that is sought. Unsurprisingly, the information concerns social relationships, the existence of possible new partners, as well as various views on the past relationship. At the same time, it becomes clear that social norms regarding this type of surveillance play an important role: "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, p. 792).

This type of passive data collection, voluntarily contributed by ex-partners on social medias, impacts, as mentioned, predominantly the individual collecting the data. However, there are cases where surveillance has gone further and come to resemble stalking. Chaulk and Jone (2011) describe several ways in which Facebook can be used for this

purpose. For example, ex-partner status updates reveal where they will be at a particular time: "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)." Another behavior might be repeatedly sending messages to the ex-partner or their friends and family, sending virtual gifts and invitations or posting comments to their ex-partners Facebook page. Grattagliano et al. also (2012) discuss stalking in digital environments and divide behaviors into three levels, where the third includes direct threats: "1) following (including showing up at the victims 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 victims 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, p. 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

Human rights in a digital environment

4 articles

The mutually shared problem as described in these articles is the relationship between individual state needs and their ambition to prevent threats against citizens on the one hand, and the problem of fundamental human rights being disregarded when the search for terrorists, for example, takes precedence, on the other hand. Obviously, this problem has its background in "911", the Bush administration's legal reaction formulated in the "USA Patriot Act" which, among other things, expanded the US government's mandate to monitor individuals' communication. McAdams (2005) formulates the tension between risks, security and basic human rights by posing the question: "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, p. 480). The same article, however, concludes that concerns for this may be unmotivated: "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, p. 495).

OBrien (2014) also addresses risks, security and human rights, with a focus on the situation in an Australian context and how children's rights are safeguarded. One problem mentioned here is that the risk (for example, of grooming) is overstated, and that the children's own capacity to consider risks and manage them are undervalued: "Foremost amongst these is that welfare discourse homogenizes 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, p. 755-756). In this context, the author proposes to view children and young people as active individuals to a greater extent, rather than passive objects whose voices must be listened to: "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, p. 771).

Hiranandani (2011) argues that the concept of terrorism is overly inclusive and is abused to justify far reaching intrusion into personal privacy. The article calls for a greater focus on the importance of considering privacy as a fundamental human right: "The post-9/11 trend seems to be towards capitalizing 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+.

OBrien, W. (2014). Australias Digital Policy Agenda. *The International Journal of Childrens 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 articles

"Sousveillance" is an interesting concept in this context, and can be described as a reaction to increased surveillance of individuals by governments and companies. The concept can be linked to the concept of Ego-Panopticism discussed in the section on general theoretical arguments above. The basic idea behind sousveillance is to flip the telescope in order to monitor the surveillant. Here, surveillance and the invasion of privacy produce a reaction and new behaviors which are expressed by citizens exposing rulers to surveillance through the use of digital technology.

Fernback (2013, p. 11) describes it as "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." Examples of tools and forums that can be used for this purpose are Facebook discussion groups (interestingly, usually directed toward the forum being used; for example, the group "Petition: Facebook, Stop Invading My Privacy" (Fernback 2013)) digitally coordinated the production and spread of videos of police violence (Bradshaw (2013), and spread surveillance films that were incriminating for the police as audio files (Ganascia 2010).

Hopes and challenges for the future: "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, p. 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

Other

5 articles

Articles that do not quite fit into any other category are presented here. Among other things, an article that introduces the concept, "Cyber-Paranoia", which describes a state of unwarranted fear of threats on the Internet (Mason et al. 2014).

Garnar (2012) addresses misuse of public computers and the ensuing need to restrict and monitor the use of them.

Park et al. (2015) describe a number of personality types related to consumer behavior on the Internet.

Lin and Lo (20105) describe a new method for collecting data-traffic and potential privacy issues related to that.

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

Behavior

There are questions that cross over into several areas and have no direct link to a specific field. An example of such a general question is the connection between how digital technology and the possibility/threat of monitoring/being monitored impacts behavior. Berger et al. (2014) state in the article "Surveillance in Digital Space and Changes in User Behavior" that the issue has not been well researched and state that "the social consequences of a comprehensive surveillance like altering the individual behavior in the digital space have hardly been studied." The study mentioned in the section "Knowl-

edge and behavior among young people", studies Internet use and behaviors and concludes that the risk of surveillance results in decreased use of the Internet.

Another article (Fuchs 2010) that discusses the same issues argues that increased information and knowledge for young people regarding privacy issues on the Internet contribute to what is known as "critical information behavior"; a concept defined as: "Critical information behavior 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, p. 180).

The article Privacy Behaviors after Snowden (Preibisch 2015) shows that although "privacy behaviors" increased following Edward Snowden's revelations of the far-reaching governmental surveillance that occurred within the framework of the PRISM program, the increase was fairly marginal and did not last very long: "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 privacy enhancing 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 Microsofts 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, p. 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 Sozialwissen-Schaftliche 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. Articles based in empirical studies sorted by method

Based in empirical studies

Of the 172 articles included in the systematic literature review, 56 articles are based in empirical findings; i.e., the articles draw conclusions on the basis of the systematic collection and analysis of data. It should be pointed out that drawing this distinction is not a simple task. Many of the articles that are not considered to be "based in empirical studies" may, for example, focus in some detail on a specific technology (see, f.ex., Lupton 2015), or the consequences of specific legislation concerning privacy (see, f.ex., Konstadinides 2011), but have not been deemed to present results based on the results of an empirical analysis. Also, many of the articles which have not been based on their own empirical data are based in previous empirical research. Among the articles based in their own empirical findings, there are slightly different approaches to data collection. The following approaches have been identified and are used to categorize the articles: surveys, interviews, case studies, mixed methods, analysis of documents, Internet logs, experimental methods and other methods.

Survey 25 articles

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

Interviews, 4 articles

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 dont 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 studies, 4 articles

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 articles

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

Analyses of documents, 2 articles

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

Internet logs, 13 articles

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

DAmbrosio, 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

Experimental, 4 articles

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

Paschaßl, 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

Other 1 article

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

Total, 56 articles

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

DAmbrosio, 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 benthams 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 dont 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

LUii is a department within Lund University dealing with digitisation from a multidisciplinary perspective.