Online Appendix—Literature Review Report

Designing for Privacy: A Design Theory for Transparency of Information Privacy Practices

Authors

- Tobias Dehling; Faculty of Management, Economics and Social Sciences; University of Cologne; Cologne; Germany
- Ali Sunyaev; Faculty of Management, Economics and Social Sciences; University of Cologne; Cologne; Germany

Literature Search

The literature review was conducted to refine the TIPP model based on extant literature. The goal of the literature review was to identify and consolidate information privacy practices deemed topically relevant for establishing transparency of information privacy practices by extant research. To focus the literature search on pertinent articles, we developed a two part search string. The first part of the search string was designed to match articles dealing with privacy policies and the second part of the search string reduced the matches to articles dealing with the content of privacy policies. Assuming that relevant articles would mention a synonym for privacy policies and a synonym for content in the title, abstract, or keywords, we restricted the literature search to matches in title, abstract, or keywords. A database search was conducted to include a wide range of outlets as well as to cover a wide range of domains. However, we restricted our search to literature databases focused predominantly on journals and conferences relevant for information systems research. Chosen databases were EBSCO (Academic Search Complete, Business Search Complete, Medline), ProQuest, AISel, and ScienceDirect. Table 1 lists the search strings formatted in the syntax of the different databases. The search strings were generated with the meta search tool LitSonar (Sturm et al. 2015). Articles were retrieved in September, 2014.

Table 1. Generic search string and database-syntax-specific search strings employed for the literature search.

Generic search string
("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications") AND ("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")
EBSCO (Academic Search Complete, Business Search Complete, Medline), ProQuest
(((TI("privacy policy" OR "privacy policies" OR "privacy statement" OR "pri-vacy statements" OR "pri-vacy notice" OR "privacy notices" OR "privacy la-bel" OR "privacy labels" OR "privacy notification" OR "privacy notifica-tions")) OR (SU("privacy policy" OR "privacy policies" OR "privacy state-ment" OR "pri-vacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "priva-cy notifications")) OR (AB("privacy policy" OR "privacy policies" OR "priva-cy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy la-bel" OR "privacy labels" OR "privacy notification" OR "privacy notifications"))) AND ((TI("content" OR "contents" OR "com-prehensive" OR "comprehensiveness" OR "element" OR "elements" OR "compo-nent" OR "components" OR "detail" OR "details" OR "composi-tion")) OR (SU("content" OR "contents" OR "comprehensive" OR "com-prehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")) OR (AB("content" OR "contents" OR "com-prehensive" OR "comprehensive-ness" OR "element" OR "elements" OR "component" OR "compo-nents" OR "detail" OR "details" OR "composition"))))
AISel
(((title:("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "pri-vacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifica-tions")) OR (subject:("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy no-tices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "privacy notifications")) OR (abstract:("privacy policy" OR "privacy poli-cies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notifi-cation" OR "privacy notifications"))) AND ((ti-tle:("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "ele-ments" OR "component" OR "components" OR "detail" OR "details" OR "composition")) OR (sub-ject:("content" OR "contents" OR "comprehen-sive" OR "comprehensiveness" OR "element" OR "ele-ments" OR "com-ponent" OR "components" OR "detail" OR "details" OR "composition")) OR (ab-stract:("content" OR "contents" OR "comprehensive" OR "compre-hensiveness" OR "element" OR "elements" OR "component" OR "compo-nents" OR "detail" OR "details" OR "composition"))))
ScienceDirect
((tak("privacy policy" OR "privacy policies" OR "privacy statement" OR "pri-vacy statements" OR "pri-vacy notice" OR "privacy notices" OR "privacy la-bel" OR "privacy labels" OR "privacy notification" OR "privacy notifica-tions")) AND (tak("content" OR "contents" OR "comprehensive" OR "com-prehensive-ness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")))

Literature Screening

To focus our research efforts, we screened all articles based on title, keywords, and abstracts. All

articles that were duplicates, not written in English, not peer-reviewed research papers, or that

did not yield any information on information on information privacy practices topically relevant for

establishing transparency of information privacy practices, were excluded from further assessment. Literature screening was independently performed by two researchers. To reduce the likelihood of false positives, we only excluded articles if both researchers unanimously identified a reason for exclusion of the article. All remaining articles were read in detail to identify information on information privacy practices topically relevant for establishing transparency of information practices.

Literature Analysis

After initial training rounds to clarify the coding scheme and resolve any misunderstandings, two researchers independently assessed 72 of the 101 remaining articles. Reliability assessment with Janson's and Olsson's ι (Janson and Olsson 2001), led to a 'substantial' (Landis and Koch 1977) and satisfactory agreement score of ι=0.72. The remaining 29 articles were assessed by one researcher. The researchers coded (Braun and Clarke 2006) all content aspects mentioned and looked especially for content aspects still missing in the TIPP model as well as any other indications for need for revisions of the TIPP model (eg, refinement of descriptions). Conflicts and ambiguities in assessments were resolved through discussions. A third researcher was consulted to resolve remaining disputes. Figure 1 illustrates all steps of literature screening and analysis in detail.
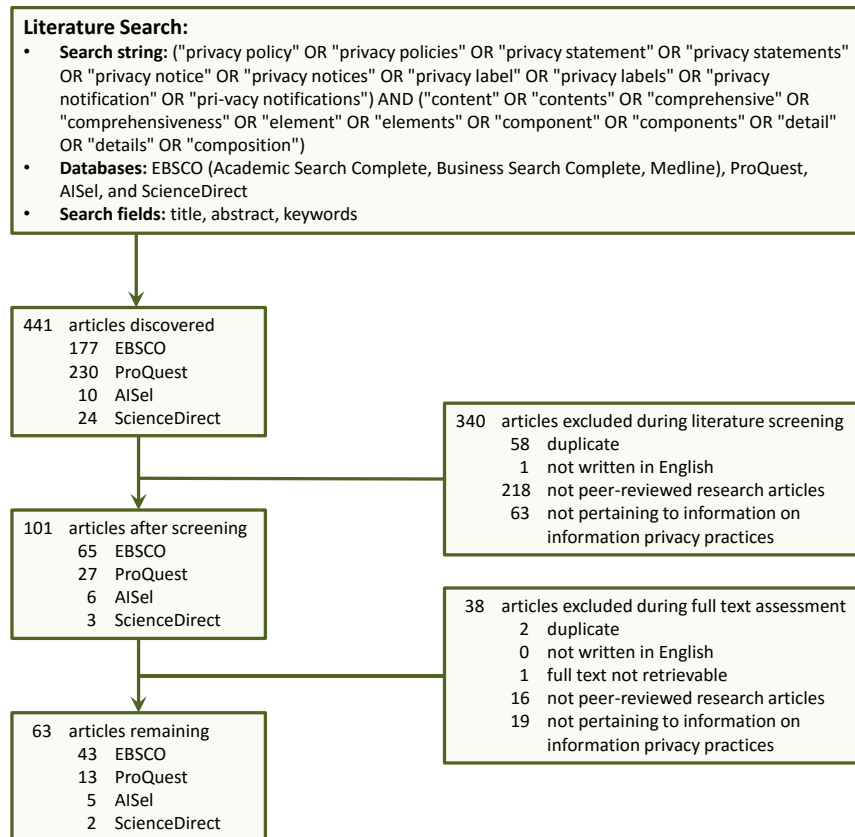
Literature Search:
- **Search string:** ("privacy policy" OR "privacy policies" OR "privacy statement" OR "privacy statements" OR "privacy notice" OR "privacy notices" OR "privacy label" OR "privacy labels" OR "privacy notification" OR "pri-vacy notifications") AND ("content" OR "contents" OR "comprehensive" OR "comprehensiveness" OR "element" OR "elements" OR "component" OR "components" OR "detail" OR "details" OR "composition")
- **Databases:** EBSCO (Academic Search Complete, Business Search Complete, Medline), ProQuest, AISel, and ScienceDirect
- **Search fields:** title, abstract, keywords

441 articles discovered
- 177 EBSCO
- 230 ProQuest
- 10 AISel
- 24 ScienceDirect

340 articles excluded during literature screening
- 58 duplicate
- 1 not written in English
- 218 not peer-reviewed research articles
- 63 not pertaining to information on information privacy practices

101 articles after screening
- 65 EBSCO
- 27 ProQuest
- 6 AISel
- 3 ScienceDirect

38 articles excluded during full text assessment
- 2 duplicate
- 0 not written in English
- 1 full text not retrievable
- 16 not peer-reviewed research articles
- 19 not pertaining to information on information privacy practices

63 articles remaining
- 43 EBSCO
- 13 ProQuest
- 5 AISel
- 2 ScienceDirect

Figure 1. Overview of literature review.

Results

Table 2 gives an overview of the discovered articles by academic discipline. The majority of discovered articles are information systems research articles (69.8%, n=44). The literature review also discovered articles from the academic disciplines law (11.1%, n=7), health sciences (6.3%, n=4), and marketing (4.8%, n=3). Other academic disciplines include computer science and philosophy.

Table 2. Discovered articles by academic discipline.

Academic discipline	Articles, N (%)
Information Systems	44 (69.8)
Law	7 (11.1)
Health Sciences	4 (6.3)
Marketing	3 (4.8)
Other	5 (7.9)

A large fraction of the articles discovered in our literature search checked information offered in artifacts communicating information privacy practices (mostly privacy policies) against predefined assessment catalogues or coding schemes (39.7%, n=25). Assessment catalogues and coding schemes were often derived from Fair Information Practices Principles (Organisation for Economic Cooperation and Development 1980; US Federal Department of Health Education and Welfare 1973) and amended with a few information privacy practices the authors were interested in. Further articles elicited what information is offered by artifacts communicating information privacy practices (17.5%, n=11) or developed normative prescriptions for information to be offered by artifacts communicating information privacy practices (12.7%, n=8). Another category of articles focused on users perceptions (eg, utility of offered information, missing information) of artifacts communicating information privacy practices (11.1%, n=7). Table 3 gives a detailed overview of the different article categories.

Table 3. Discovered articles by article category.

Article category	Category description	Articles, N (%)
Content Assessment	Articles assessing the information offered by artifacts (eg, privacy policies, privacy seals) communicating information privacy practices against a predefined assessment catalogue/coding scheme.	25 (39.7)
Content Analysis	Articles examining what information is offered by artifacts (eg, privacy policies, privacy seals) communicating information privacy practices.	11 (17.5)
Content Prescription	Articles making normative prescriptions what information should be offered in artifacts (eg, privacy policies, privacy seals) communicating information privacy practices.	8 (12.7)
User Perception	Articles studying user perceptions of artifacts (eg, privacy policies, privacy seals) communicating information privacy practices.	7 (11.1)
User Concerns	Articles eliciting users' information privacy concerns, thereby, revealing information privacy practices of interest to users.	3 (4.8)
Other	Other articles focus on issues like effective design of artifacts communicating information privacy practices or user preferences for information on information privacy practices.	9 (14.3)

In this work, we used the term 'privacy policy' to refer to the text documents posted on information system providers' web sites and detailing their information privacy practices. Extant literature does not employ a common terminology to refer to privacy policies (Table 4). 42 articles (66.7%) use the term 'privacy policy', 8 articles (12.7%) use the term 'privacy notice, 7 articles (11.1%) use the term 'privacy statement', and 4 articles (6.3%) used the term privacy policy statement. Some articles employ multiple terms interchangeably to refer to privacy policies.

Table 4. Terminology used to refer to privacy policies in the articles in our sample. Percentages do not sum up to 100% because a few articles use multiple terms interchangeably. *'Not applicable' refers to articles that did not address privacy policies.

Term	Articles, N (%)
Privacy policy	42 (66.7)
Privacy notice	8 (12.7)
Privacy statement	7 (11.1)
Privacy policy statement	4 (6.3)
Not applicable*	2 (3.2)

During the literature analysis we identified X content aspects. We organized identified content aspects in a hierarchy. The root node is 'Content'. Nodes on deeper tiers in the hierarchy refine their parents. To structure the first tier, we used major information privacy concerns, information collection, handling of information, rationale for information privacy practices, and offered privacy controls (Ackerman et al. 1999; Antón et al. 2010; Earp et al. 2005). An additional content aspect on the first tier captures meta-information (eg, provider name, contact information), which is not directly related to information privacy. The maximum depth of the hierarchy is 5. Table X outlines the hierarchy, lists all content aspects with a detailed description, states how often a content aspect was mentioned by articles in our sample, and indicates during which stage of our research approach the content aspect was added.

By design, content aspects capture relevant content for information system providers' communications of their information privacy practices. Hence, content aspects do not offer detailed infor-

mation whether and how information privacy practices are implemented by the information systems provider. To capture such knowledge as well, we added a companion model representing practice aspects. The root node is 'Practice'. Nodes on deeper tiers represent different facets of information privacy practices. The practice aspect 'ExecutionPractice' is widely applicable and captures, for example, whether an information privacy practices is always carried out, not carried out, or only carried out with explicit consent or until users revoke implicit consent. A more focused The practice aspect 'RetentionPractice' is more focused and characterizes, for instance, whether information is only retained as long as the stated purposed for information collection are met, until legal requirements for retention are fulfilled, or as long as the information system provider desires.

Modelled after properties in ontologies (Noy and McGuinness 2001), relationships between content aspects and practice aspects are represented through dedicated content aspects named after the respective practice aspect prefixed with 'has'. For example, the content aspect 'InformationSharingContent' has the child content aspects 'hasExecutionPractice' and 'hasProtectionPractice'. Thus, 'ExecutionPractice' practice aspects can be used to capture whether information is shared with certain potential recipients and 'ProtectionPractice' practice aspects can be used to indicate whether and how the information recipient protects the information (eg, according to own information privacy practice, with the same protection level as the data collector, or with a protection level at least as high as the protection level of the data collector. For the sake of parsimony, content aspects expressing relationships between content aspects and practice aspects are inherited. Hence, the child content aspect 'hasExecutionPractice' of the tier-1 content aspect 'InformationCollectionContent' represents also relationships for the child content aspects on tier-2 to tier-5.

Hierarchy				Content aspect	Added	# Articles	Description
C				Content	P3P review		Information to be offered by artifacts communicating information on information privacy practices
C	H			HandlingOfInformationContent	P3P review		Captures how the information system handles information
C	H	1		InformationRetentionContent	P3P review		Information retention practices of the information system provider
C	H	1	1	hasExecutionPractice	App review		Captures whether information retention practice is carried out
C	H	1	2	hasRetentionPractice	App review		Captures how information is retained
C	H	2		InformationSecurityContent	App review		High-level information on information security measures
C	H	2	1	SecurityDuringProcessingContent	App review		Information security measures protecting information during processing
C	H	2	2	SecurityDuringStorageContent	App review		Information security measures protecting information in rest
C	H	2	3	SecurityDuringTransferContent	App review		Information security measures protecting information in transfer
C	H	3		InformationSharingContent	P3P review		Captures with whom information is shared
C	H	3	1	hasExecutionPractice	App review		Captures whether information sharing practice is carried out
C	H	3	2	hasProtectionPractice	P3P review		Captures how shared information is protected in recipients' information system relative to provider information system
C	H	3	3	SharingWithAdvertiserContent	App review		Information sharing with third party that offers advertising services within provider information system or on their own
C	H	3	4	SharingWithAggregatorContent	Lit review		Information sharing with data aggregators (ie, entities that compile data bases, usually drawn from various information sources and then, for example, sold for marketing purposes)
C	H	3	5	SharingWithAnalystContent	App review		Information sharing with third party that runs analysis services for the information system provider (eg, compilation of usage statistics)
C	H	3	6	SharingWithDeliveryContent	P3P review		Information sharing with third parties performing physical delivery services
C	H	3	7	SharingWithGovernmentContent	P3P review		Information sharing with government agencies
C	H	3	8	SharingWithOtherUsersContent	App review		Information sharing with other users of the information system
C	H	3	9	SharingWithProviderAgentsContent	P3P review		Information sharing with provider agents that process data only on behalf of the information system provider
C	H	3	10	SharingWithPublicContent	P3P review		Information sharing with the public
C	H	3	11	SharingWithUnrelatedContent	P3P review		Information sharing with unrelated third parties not involved in service provision
C	H	3	12	SharingWithUserAuthorizedContent	App review		Information sharing with third parties authorized by the user

C								
C	H	4			InformationStorageContent	App review		Captures where information is stored
C	H	4	1		hasExecutionPractice	App review		Captures whether information storage practice is carried out
C	H	4	2		CloudStorageContent	App review		Data stored in the cloud
C	H	4	3		LocalStorageContent	App review		Data stored on the user device accessing the information system
C	H	4	4		OtherUserDeviceStorageContent	App review		Data stored on secondary user device (eg, personal computer, flashdrive)
C	H	4	5		ProviderStorageContent	App review		Data stored within information system provider's domain
C	H	4	6		ThirdPartyStorageContent	App review		Data stored by a third party storage service
C	I				InformationCollectionContent	App review		Captures what and how information is collected
C	I	1			hasExecutionPractice	Lit review		Captures whether information collection practice is carried out
C	I	2			InformationCollectionSensorContent	App review		Sensors used to collect information, the sources of collected information
C	I	2	1		EnvironmentSensorContent	App review		Sensors collecting information on the device (the user) environment
C	I	2	1	1	BluetoothSensorContent	App review		Discover contactable bluetooth-enabled devices
C	I	2	1	2	CameraContent	App review		Collect images/videos made with the device camera
C	I	2	1	3	MicrophoneContent	App review		Collect sound recordings made with the microphone of the device
C	I	2	1	4	NearFieldCommunicationContent	App review		Record user actions (eg, payments) conducted via Near Field Communication (NFC)
C	I	2	2		LocationSensorContent	App review		Sensors for location information
C	I	2	2	1	GpsSensorContent	App review		GPS location of the device
C	I	2	2	2	NetworkConnectionSensorContent	App review		Location coordinates based on cell towers or other network identifiers (eg, IP address)
C	I	2	2	3	WiFiSensorContent	App review		Location coordinates based on available WiFi networks
C	I	2	3		UserSensorContent	App review		Sensor collecting information on the user
C	I	2	3	1	FingerprintScannerContent	App review		Collection of users' fingerprint with fingerprint scanner
C	I	2	4		SoftwareUseSensorContent	Lit review		Sensors collecting information on software use/perception
C	I	2	4	1	AdwareContent	Lit review		Collection through adware installed on the device
C	I	2	4	2	CookiesContent	P3P review		Collection through cookies
C	I	2	4	3	SurveysContent	P3P review		Collection with surveys or questionnaires
C	I	2	4	4	TrackingSoftwareContent	Lit review		Collection with tracking software installed on the device
C	I	2	4	5	WebBeaconContent	Lit review		Tracking of user activity through web beacons (eg, what information system content was accessed)

C	I	3			InformationCollectionTypeContent	P3P review		Type of collected information
C	I	3	1		InformationFormContent	Lit review		Different forms of data collected
C	I	3	1	1	AudioInformationContent	Lit review		Collection of audio data
C	I	3	1	2	ImageInformationContent	Lit review		Collection of image/photo data
C	I	3	1	3	MetaDataContent	Lit review		Collection of meta-data (data on data; eg, geo tags in photos)
C	I	3	1	4	TextInformationContent	Lit review		Collection of textual data
C	I	3	1	5	VideoInformationContent	Lit review		Collection of video data
C	I	3	2		IdentifierContent	App review		Collection of user identifiers
C	I	3	2	1	FinancialIdentifierContent	App review		Financial identifiers (eg, bank account or credit card number)
C	I	3	2	2	GovernmentIdentifierContent	P3P review		Government-issued identifiers (eg, social security number)
C	I	3	2	3	NameContent	Lit review		Collection of users full name (not usernames)
C	I	3	2	4	OnlineContactContent	P3P review		Information that allows to contact the user on the internet
C	I	3	2	5	PhysicalContactContent	P3P review		Information that allows to contact the user in the physical world (eg, postal addresse, phone number)
C	I	3	2	6	OwnUniqueIdentifierContent	P3P review		Identifiers issued by the information system provider for purposes of consistently identifying users (eg, usernames)
C	I	3	3		OperationalContent	App review		Information collected for information system operation
C	I	3	3	1	CommunicationsContent	P3P review		Words and expressions contained in the body of a communication (eg, emails, bulletin board postings, chat room entries)
C	I	3	3	2	InteractionContent	P3P review		Data actively generated from or reflecting explicit interactions with a provider information system (eg, queries to a search engine, or logs of account activity)
C	I	3	3	3	LocationContent	P3P review		Information that identifies users' current physical location (eg, GPS position data)
C	I	3	3	4	NavigationContent	P3P review		Data passively generated by information system use (eg, information retrieved and time spent)
C	I	3	3	5	OnlineContactsContent	P3P review		Online contact information of other users to facilitate communication
C	I	3	3	6	PurchasesContent	P3P review		Information actively generated by purchases conducted within the information system
C	I	3	4		UserDetailsContent	App review		Information on the user
C	I	3	4	1	DemographicsContent	P3P review		Demographic and socioeconomic data

C	I	3	4	2	FinancesContent	P3P review		Information on users' finances (eg, account balance, payment or overdraft history)
C	I	3	4	3	HealthContent	P3P review		Information about users' physical or mental health, sexual orientation, and use of or inquiry into health care services or products
C	I	3	4	4	IdeologicalContent	P3P review		Affiliations with groups (eg, religious organizations, trade unions, professional associations, political parties)
C	I	3	4	5	PreferencesContent	P3P review		Information about users' likes and dislikes (eg, favorite color)
C	I	3	4	6	UserDeviceContent	P3P review		Information about user client device (eg, IP address, domain name, browser type, or operating system)
C	M				MetaContent	App review		Content aspects that are not directly related to information privacy practices
C	M	1			CertificationContent	App review		Certifications of the information system/the information system provider
C	M	2			ContactContent	Lit review		Contact information of information system provider
C	M	3			EffectiveDateContent	Lit review		Date from which onwards the stated information privacy practices are in effect
C	M	4			FollowedGuidelinesContent	App review		Guidelines the information system provider followed
C	M	5			FollowedLawsContent	App review		Laws the information system provider or the information system is compliant with
C	M	6			LastUpdateContent	Lit review		Date of the last time the stated privacy practices were updated
C	M	7			MinimumUserAgeContent	Lit review		Outlines the targeted age group (especially important to ascertain whether children are targeted)
C	M	8			ProviderNameContent	Lit review		Name of the information system provider and further information on provider entity
C	O				OfferedPrivacyControlContent	App review		Captures offered privacy controls
C	O	1			AccessAuditContent	App review		Enable users to retrieve access logs for their information.
C	O	1	1		hasExecutionPractice	App review		Captures whether users can retrieve access logs for their information
C	O	2			BreachNotificationContent	App review		Captures how users are notified about breaches of information privacy
C	O	2	1		hasNotificationPractice	Lit review		Captures whether users are notified about breaches
C	O	2	2		BreachNatureContent	App review		Notification about what was breached
C	O	2	3		BreachOccurenceContent	App review		Notification that a breach occurred
C	O	2	4		BreachRemediesContent	App review		Notification about remedies offered for breach
C	O	3			ChangeHistoryContent	Lit review		Information on past information privacy practices and performed changes

C	O	4		ChangeGovernanceContent	Lit review		Explains how changes in information privacy practices reflect on already collected information
C	O	4	1	hasChangeGovernancePractice	Lit review		Captures the change governance practices carried out
C	O	5		ChangeNotificationContent	P3P review		Notification about changes of information privacy practices
C	O	5	1	hasNotificationPractice	App review		Captures whether and how users are informed about changes of information privacy practices
C	O	6		ConsentManagementContent	P3P review		Illustrates all consents, explicit and implicit, and enables users to revoke and modify given consents
C	O	7		DisputeRemedyContent	P3P review		Remedies offered for justified disputes regarding information privacy practices
C	O	7	1	hasDisputeRemedyPractice	Lit review		Captures remedies offered for justified disputes regarding the information privacy practices
C	O	8		DisputeResolutionContent	P3P review		Means offered for resolving disputes regarding information privacy practices
C	O	8	1	hasDisputeResolutionPractice	Lit review		Captures means offered for resolving disputes regarding the information privacy practices
C	O	9		DownstreamPropagationContent	Lit review		Describes how changes of information, especially, corrections and deletions of user information made by users, are communicated with and propagated to any third party with which the data was shared
C	O	9	1	hasImplementationPractice	Lit review		Captures whether downstream propagation practices are implemented
C	O	10		PrivacyManagementBoundariesContent	App review		Captures the boundaries for information privacy management (eg, information requests by law enforcement, control of information privacy practices of subsidiaries)
C	O	11		PrivacyPracticeMonitoringContent	Lit review		Describes how the actual information privacy practices of the information system provider are monitored
C	O	11	1	hasImplementationPractice	Lit review		Captures whether monitoring practices for information privacy practices are implemented
C	O	11	2	AutomatedMonitoringContent	Lit review		Automated monitoring of information privacy practices (eg, by some software)
C	O	11	3	IndependentMonitoringContent	Lit review		Monitoring of information privacy practices by an independent party
C	O	11	4	InternalMonitoringContent	Lit review		Monitoring of information privacy practices by the information system provider
C	O	12		SecondaryUseConsentContent	Lit review		Describes how users are contacted for affirmative consent (opt-in) prior to any secondary use (ie, use of user information for any purpose other than for which it was collected)

C	O	12	1	hasImplementationPractice	Lit review		Captures whether practices for secondary use consent are implemented
C	O	12	2	hasNotificationPractice	Lit review		Captures whether and how users are notified about secondary uses of their information
C	O	13		UserAccessContent	App review		Captures what permissions users' have to access information collected on them
C	O	13	1	hasAccessRightsPractice	App review		Captures acccess rights of users for information collected on them
C	P			PracticeRationaleContent	P3P review		Captures for what purposes information privacy practices are performed
C	P	1		hasExecutionPractice	App review		Captures whether information privacy practices are carried out for the given purposes
C	P	2		CommunicationContent	App review		To provide communication features
C	P	2	1	ContactContent	P3P review		Responding to the user (eg, respond to user query, provide users with feedback)
C	P	2	2	FeedbackContent	P3P review		Contacting users without previous request by users
C	P	2	3	MarketingContent	P3P review		Advertising, marketing, or promotion purposes
C	P	2	4	UserCommunicationContent	P3P review		Facilitating communication between users
C	P	3		OfferedServiceContent	App review		To provide services offered by the information system
C	P	3	1	FinancialManagementContent	P3P review		Banking and financial management
C	P	3	2	HealthProductsContent	P3P review		To offer users products or services that relate to their physical or mental health
C	P	3	3	PaymentContent	P3P review		Payment and transaction facilitation, the information system provider is the one processing the payment
C	P	3	4	PhysicalDeliveryContent	P3P review		Physical delivery of a product
C	P	3	5	SalesContent	P3P review		Conducting a business transaction with the user (eg, completing a sale)
C	P	4		PersonalizationContent	App review		Personalization of the information system
C	P	4	1	IndividualAnalysisContent	P3P review		To determine the habits, interests, or other characteristics of users and combine it with identified data for the purpose of research, analysis, and reporting
C	P	4	2	IndividualDecisionContent	P3P review		To determine the habits, interests, or other characteristics of individuals and combine it with identified data to make a decision that directly affects that individual
C	P	4	3	PseudoAnalysisContent	P3P review		To determine the habits, interests, or other characteristics of users for purposes of research, analysis, and reporting based on pseudonymous identifiers

C	P	4	4	PseudoDecisionContent	P3P review		To determine the habits, interests, or other characteristics of individuals to make a decision that directly affects that individual based on pseudonymous identifiers
C	P	5		PublicWelfareContent	App review		To contribute to public welfare
C	P	5	1	ArtsContent	P3P review		For delivering the arts (eg, music, literature, movies)
C	P	5	2	CharityContent	P3P review		For charitable purposes
C	P	5	3	EducationContent	P3P review		For educational purposes
C	P	5	4	GovernmentContent	P3P review		For online government services (eg, voter registration, citizen information services)
C	P	5	5	HistoricalContent	P3P review		For the purpose of preserving social history
C	P	5	6	ResearchContent	P3p review		To support research projects
C	P	6		ServiceOperationContent	App review		To operate the information system
C	P	6	1	CoreFunctionalityContent	P3P review		To conduct and support activities for which data was provided
C	P	6	2	AdministrationContent	P3P review		For information system administration
C	P	6	3	DevelopmentContent	P3P review		To enhance, evaluate, or review the information system
C	P	6	4	LegalObligationsContent	P3P review		To fulfill duties enforced by law (eg, court proceedings) or for other legal purposes
C	P	7		TechnicalDetailsContent	App review		For technical purposes
C	P	7	1	AccountManagementContent	P3P review		For user account management
C	P	7	2	SessionManagementContent	P3P review		To keep track of sessions and application state
P				Practice	Lit review		Captures manifestations of information privacy practices
P	1			AccessRightsPractice	App review		Captures user access rights
P	1	1		View	App review		Users can view information collected on them
P	1	2		Correct	Lit review		Users can correct/modify/update information collected on them
P	1	3		Download	App review		Users can download information collected on them
P	1	4		Delete	App review		Users can delete information collected on them
P	1	5		Pseudo-Delete	App review		Users can delete information collected on them, but the information system provider may keep a copy (eg, in backups or to comply with legal obligations)
P	1	6		View+Correct	App review		Users can view and correct information collected on them
P	1	7		View+Delete	App review		Users can view and delete information collected on them
P	1	8		View+Download	App review		Users can view and download information collected on them

P	1	9	View+Correct+Delete	App review		Users can view, correct, and delete information collected on them
P	1	10	View+Delete+Download	App review		Users can view, correct, and download information collected on them
P	1	11	View+Correct+Delete+Download	App review		Users can view, correct, delete, and download information collected on them
P	1	12	No-Access	App review		Users have no access to information collected on them
P	1	13	Unspecified	App review		User access rights are unspecified
P	2		ChangeGovernancePractice	Lit review		Captures how changes in information privacy practices reflect on already collected information
P	2	1	MostCurrentPractices	Lit review		Information is treated according to the current information practices
P	2	2	PracticeAtCollection	Lit review		Information is treated according to the information privacy practices in place at time of information collection
P	2	3	Unspecified	Lit review		Change governance practices are unspecified
P	3		DisputeRemedyPractice	Lit review		Captures remedies for justified disputes regarding providers' information privacy practices
P	3	1	Correct	P3P review		Justified disputes regarding providers' information privacy practices are remedied through rectification of errors or consequences
P	3	2	Law	P3P review		Justified disputes regarding providers' information privacy practices are remedied as specified by law
P	3	3	Money	P3P review		Justified disputes regarding providers' information privacy practices are remedied through monetary compensations
P	3	4	No-Remedy	App review		Justified disputes regarding providers' information privacy practices are not remedied
P	3	5	Unspecified	Lit review		Remedies offered for justified disputes regarding providers' information privacy practices are unspecified
P	4		DisputeResolutionPractice	Lit review		Captures practice in place to resolve disputes
P	4	1	Applicable-Law	P3P review		Disputes are resolved as enshrined in law
P	4	2	Court	P3P review		Disputes are resolved in front of court
P	4	3	Customer-Service	P3P review		Customer service resolves disputes
P	4	4	Independent-Organization	P3P review		A third-party organization resolves disputes
P	4	5	No-Resolution	App review		No means are offered for resolving disputes
P	4	6	Unspecified	Lit review		Means offered for resolving disputes are unspecified
P	5		ExecutionPractice	P3P review		Captures whether a practice is carried out
P	5	1	Always	P3P review		Practice is always carried out

P	5	2	Never	App review		Practice is and will never be executed
P	5	3	Not-Executed	App review		Practice is not executed
P	5	4	Not-Now	App review		Practice is not executed but might be executed in the future
P	5	5	Not-Required	Lit review		Alternative means for IS artifact use are offered so that the practice can be avoided
P	5	6	Opt-In	P3P review		Practice is not carried out without explicit consent
P	5	7	Opt-Out	P3P review		Practice is carried out as long as users do not revoke implicit consent
P	5	8	Unspecified	App review		It is unspecified whether the practice is executed
P	6		ImplementationPractice	App review		Captures whether a practice is implemented
P	6	1	Implemented	App review		Practice is implemented
P	6	2	Partially-Implemented	App review		Practice is partially implemented
P	6	3	Not-Implemented	App review		Practice is not implemented
P	6	4	Unspecified	App review		It is unspecified whether the practice is implemented
P	7		NotificationPractice	App review		Captures whether and how users are notified
P	7	1	On-Next-Access	App review		Users are notified the first time they use the IS artifact after notification was initiated
P	7	2	User-Notified-By-Mail	App review		Users are notified by mail
P	7	3	Mail-And-Next-Access	App review		Users are notified by mail and on their next access of the IT artifact
P	7	4	No-Notification	App review		Users are not notified
P	7	5	Unspecified	App review		It is unspecified whether and how users are notified
P	8		ProtectionPractice	P3P review		Captures how shared information is protected in recpients' information system relative to provider information system
P	8	1	Not-Lower	App review		The recipient is bound to handle the information with a level of information privacy that is not lower than the level offered by the provider
P	8	2	Recipients	P3P review		The recipient handles the information according to own information privacy practices
P	8	3	Same	P3P review		The recipient is bound to handle the information with the same level of information privacy as the provider
P	8	4	Unspecified	P3P review		It is unknown how shared information is protected
P	9		RetentionPractice	Lit review		Captures how information is retained
P	9	1	Business-Practices	Lit review		Information is retained according to common or widely-used business practices

P	9	2	Indefinitely	Lit review		Information is retained for an indeterminate period of time. Information is retained until the provider wants it deleted.
P	9	3	Legal-Requirement	Lit review		Information is retained as long as required by law
P	9	4	Stated-Purposes	Lit review		Information is retained to meet the stated purpose and discarded at the earliest time possible
P	9	5	User-Preference	Lit review		Information is retained until the user wants it deleted
P	9	6	No-Retention	Lit review		Information is not retained for more than a brief period of time necessary to make use of it during the course of a single online interaction.
P	9	7	Unspecified	Lit review		It is unspecified whether or how information is retained

Table Y gives an overview of the articles in our final sample and lists all 63 articles with a brief outline of the article aims, and the number of content aspects and practice aspects mentioned in the paper. During literature analysis, we also coded whether content aspects were deemed relevant or irrelevant for transparency of information privacy practices. However, none of the articles in our sample characterized any content aspects as irrelevant. Hence, all content aspects mentioned in papers were considered relevant for transparency of information privacy practices. We only excluded content aspects that were incidentally mentioned in sample articles. Content aspects were, for example, coded as relevant for transparency of information privacy practices if articles state that users should be information about them, use them in coding schemes, state that users are concerned about them, or if articles reported that content aspects were deemed relevant in pertinent legal proceedings.

Reference	Academic discipline	Category	Article aims	# content aspects	# practice aspects
(Fang 2010)	Law	Content pre-scription	Discusses a case where the privacy policy offered by the US retailer Sears was determined to be deceptive by the Federal Trade Commission and recommends five measures for effective privacy disclosures		
(Wu et al. 2012)	Information Systems	Impact quantitative	Investigates why consumers with different cultures react differently to the content of various privacy policies which may influence their trust or willingness to provide personal information		
(Weitzman et al. 2011)	Health	Content assessment	To foster informed decision-making about health social networking by patients and clinicians the authors evaluated the quality/safety of SN sites policies and practices		
(Unruh et al. 2004)	Health	Content pre-scription	The objectives of this study were to identify women's preferences for receiving online breast cancer risk information, to identify barriers to accessing this information, and to identify differences in these factors between internet users and non-users		
(Tsai et al. 2011)	Information Systems	User perception study	Determines whether a more prominent display of privacy information will cause consumers to incorporate privacy considerations into their online purchasing decisions		
(Timpson and Troutman 2009)	Marketing	Privacy policy design	Investigates the lack of real standards or specifications as to how privacy policies should be issued and what specific content should be included		
(Tavani 2007)	Philosophy	Content pre-scription	Articulates a definition of information privacy that can serve as a foundation for a theory of information privacy and shows how this theory enables 0online privacy policies that are clear transparent and consistent		
(Suominen 2012)	Health	Content pre-scription	Aims to better understand the requirements for using health data in research internationally by comparing international Australian and Finnish frameworks		

(Strickland and Hunt 2005)	Information Systems	Content pre-scription	Investigates whether the public understands RFID technologies and the manner in which personally identifiable information may be collected main-tained used and disseminated and whether the public consents to these information practices		
(Stanaland et al. 2009)	Information Systems	Content assess-ment	Examines how differences in regulatory infor-mation privacy environments manifest in privacy information offered to parents on children's web sites in the US and UK		
(Schwaig et al. 2006)	Information Systems	Content assess-ment	Examines the privacy practices and policies of the Fortune 500 in order to assess how well their pri-vacy policies adhere to fair information practice principles, develops a way to analyze the maturity level of firms with respect to their information pri-vacy disclosure, and determines the extent and substance of online privacy disclosure among the largest and most influential US firms		
(Schuele 2005)	Information Systems	Content assess-ment	Assesses the degree to which cities address is-sues of privacy on their websites		
(Savirimuthu 2013)	Law	None	Clarifies the content and application of data pro-tection and privacy rights and outlines a policy framework that will address the lack of specificity on how innovation and privacy issues can be bet-ter calibrated.		
(Rains and Bosch 2009)	Health	Content assess-ment	Reports a content analysis of the privacy policies from 97 general reference health web sites that was conducted to examine the ways in which visi-tors privacy is constructed by health organizations		
(Proctor et al. 2008)	Information Systems	User perception study	Examines the types of information solicited by dif-ferent categories of web sites and whether users are able to comprehend a sites privacy policy to reveal whether the requested information varies within and between different categories of sites and whether it is necessary for the site to com-plete a transaction or provide a service		
(Pollach 2007)	Information Systems	Content analysis	Investigates why privacy policies fail to effectively communicate data handling practices		

(Pollach 2006)	Information Systems	Content analysis	Examines systematically what data handling practices companies engage in, which ones they do not engage in, and whether they fail to address important areas of concern to users		
(Peslak 2005)	Information Systems	Content assessment	Provides a background on internet privacy, summarizes prior internet privacy studies, updates and expands on internet privacy studies, and proposes an expanded factor analysis as a guide for future studies		
(Papacharissi and Fernback 2005)	Information Systems	Content analysis	Evaluates the overall efficacy of privacy policies and focuses on the language, format, privacy reassurances, complexity of legal and technical terms, and perceived statement credibility		
(O'Connor 2003)	Information Systems	Content assessment	Assesses whether hotel web sites collect personal information and what reassurances they give customers about what will be done with their personal data, whether hotel web sites display privacy policies and conform to international norms, whether hotel web sites make use of trust marks or privacy seals, and whether hotel web sites conform to their stated privacy policies		
(Mundy 2006)	Information Systems	Content assessment	Analyzes privacy policies on popular UK healthcare-related web sites to determine the extent to which consumer privacy is protected		
(Milne and Culnan 2002)	Information Systems	Content assessment	Addresses methodological issues related to using surveys of online privacy policies in the public policy process to evaluate the voluntary posting of privacy policies and the extent to which these disclosures are based on fair information practices		
(Metzger 2006)	Information Systems	User perception study	Explores how characteristics of online vendors and consumers interact with web site communications to affect consumer behavior online		
(Magi 2010)	Information Systems	Content assessment	Assesses whether vendors collect user information and handle that information in accordance with privacy standards articulated by the library profession and the information technology industry		

(LaRose and Rifon 2006)	Information Systems	Content assessment	Examines whether website proprietors are tacitly following a theory of privacy behavior that assumes that website proprietors have an interest in collecting consumer information and that consumer disclosure of personal information is often the currency of exchange to obtain the desired outcomes at a website		
(Langenderfer and Cook 2004)	Law	None	Examines different regulatory mechanisms that protect privacy and their strengths and weaknesses		
(Kuzma 2011)	Information Systems	Tool-supported privacy feature crawl	Analyzes the level of privacy protection among 60 major online social networks throughout the world		
(Kubis 2010)	Law	Content prescription	Proposes a solution to the privacy concerns raised by services like Google Books		
(Kim and Yi 2010)	Information Systems	Content analysis	Enquires how children-targeting commercial sites endeavor to protect personal information and how children face the possibility of personal information exposure on the web, and discusses a plan to reduce the risk of privacy invasion		
(Kaupins and Reed 2012)	Information Systems	Content analysis	Examines how new media and privacy policies have penetrated the top twelve online newspaper websites in the Baltic States, Estonia, Latvia, and Lithuania		
(Shalhoub 2006)	Information Systems	Content assessment	Evaluates the contents of privacy policies from a sample of Gulf Cooperation Council companies engaged in electronic commerce transactions		
(Hong et al. 2005)	Information Systems	Content assessment	Explores the information collection practices and privacy policies of online news sites		
(Xu et al. 2011)	Information Systems	User perception study	Explores the link between individual privacy perceptions and institutional privacy assurances		
(Garrison et al. 2012)	Information Systems	Privacy policy design	Identifies barriers to consumer understanding of privacy policies and develops an alternative privacy policy design that consumers could more easily understand and use		
(Faja and Trimi 2006)	Information Systems	User concerns	Attempts to answer the question of whether having more privacy-related elements in the web site results in better perceptions of information privacy which in turn would result in a greater willingness to disclose information and buy from the site		

(Desai et al. 2012)	Law	Content pre-scription	Reviews FTC enforcement actions especially as they relate to the commissions recently released Privacy Report and provides a set of practical tips and best practices to assist businesses in staying aligned with these emerging trends in consumer privacy protection		
(Culnan 2000)	Marketing	Content assessment	Assesses the extent to which 361 consumer-oriented commercial Web sites post disclosures that describe their information practices and whether these disclosures reflect fair information practices		
(Cottrill 2011)	Information Systems	None	Attempts to provide a clear review of the methods by which privacy protection may take place at the levels of law, technology, and management		
(Liu and Arnett 2002)	Information Systems	Content assessment	Examines web sites of the Global 500 and shows that different countries greatly vary in their use of privacy policies on their web sites and their use of seal programs as visible signs of attention to privacy concerns		
(Cai et al. 2003)	Information Systems	Content pre-scription	Examines the amount and types of personal information collected from children online in October 2000, approximately two years after COPPA was passed by Congress and six months after implementation, and assesses the degree to which website providers complied with COPPA rules		
(Beldad et al. 2009)	Information Systems	Content assessment	Dissects the contents of privacy policies on municipal websites and determines whether the contents of privacy policies on Dutch municipal websites coincide with the significant provisions in the Wet Bescherming Persoonsgegevens		
(Ashrafi and Kuil-boer 2005)	Information Systems	Content assessment	Examines privacy issues in the context of fair information practices and how they are perceived and practiced by the top 500 interactive companies in the United States		
(Almatarneh 2011)	Information Systems	Content assessment	Assesses and evaluates the level to which the privacy of personal information is maintained and protected in Jordan		

(Stitilis and Ma-linauskaite 2013)	Law	Content assess-ment	Analyzes the compliance with basic principles of data protection in selected consumer-oriented cloud services contracts and highlights the ade-quate level of data protection in the mentioned contracts		
(Cha 2011)	Information Systems	Content assess-ment	Investigates the depth of personal information that web proprietors collect from consumers in con-junction with the privacy policies of their sites		
(McGrath 2011)	Information systems	Users' content preferences	Gathers information about the importance of pri-vacy policies and their contents on social network-ing web sites		
(Hooper and Evans 2010)	Information systems	Content assess-ment	Analyses the terms of use and privacy statements of six social networking sites against the agreed national values on information handling promul-gated in the New Zealand Privacy Act of 1993		
(Kuzma 2010)	Information Systems	Content assess-ment	Analyses the level of privacy protection among 50 US Senate web sites		
(Hooper and Vos 2009)	Information Systems	Content assess-ment	Examines the extent to which New Zealand busi-ness web sites conform to the provisions of the New Zealand Privacy Act, 1993 as an articulation of the national values on the rights of individuals to information privacy		
(Ciocchetti 2007)	Law	Content pre-scription	Proposes a new federal law designed to make electronic privacy polices more effective		
(Zhang et al. 2007)	Information Systems	Content assess-ment	Examines the leading international companies' online privacy policies, particularly of firms that are on Forbes' Global 2000 list		
(McRobb 2006)	Information systems	User perception study	Investigates how readers understand the meaning of a small set of privacy policies		
(Meinert et al. 2006)	Information systems	User perception study	Examines the willingness of individuals to provide various types of information based on varying lev-els of protection offered by privacy policies		
(Schwaig et al. 2005)	Information systems	Content analysis	Examines the reasons for firms to invest organiza-tional resources in a consumer protection mecha-nism that consumers rarely access and the rea-sons why researchers rely on compliance to fair information practices as a measure of whether or not self-regulation is working and as a surrogate for consumers' protection		

(McRobb and Rogerson 2004)	Information Systems	Content assessment	Surveys privacy policies to reach a better understanding of privacy policies on the internet and the interplay between these policies and other factors.		
(Wijnholds 2001)	Marketing	None	Explores legal and environmental issues with respect to privacy, security, taxation, and liability		
(Yee and Korba 2013)	Computer Science	Content prescription	Presents two semi-automated approaches for obtaining personal privacy policies for consumers		
(Hossain and Dwivedi 2014)	Information Systems	User concerns	Explores the catalysts of perceived privacy taking RFID as a representative technology and applying it in national applications		
(Hooper et al. 2007)	Information Systems	Content analysis	Explores whether privacy principles might be applied as a basis for assessing banking websites for responsible business practice in electronic commerce		
(Rizk et al. 2010)	Information Systems	Content analysis	Studies the privacy concerns of SNS providers with respect to users and other stakeholders, to understand how these topics are related to each other in the documents, and studies the construction of the different roles, responsibilities and accountabilities assigned to the different stakeholders		
(Robles-Estrada et al. 2006)	Information Systems	Content assessment	Explores and analyzes the content of 120 privacy statements from online companies established in Mexico to address all privacy dimensions that seem to be important in online environment		
(Clarke 2006)	Information Systems	Content assessment	Evaluates privacy policies against a normative template in order to assess the extent to which they are likely to represent effective protection for consumers' privacy		
(Bulgurcu et al. 2010)	Informaton Systems	User perception study	Investigates what users' perceived privacy issues are in an online social networking site, what triggers users' attribution of an informational practice to a privacy issue, and what are outcomes of users' perceived privacy issues		

References

Ackerman, M. S., Cranor, L. F., and Reagle, J. 1999. Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. *1st ACM Conference on Electronic Commerce*EC-99. 1–8.

Almatarneh, A. 2011. Privacy Implications for Information and Communications Technology (ICT): The Case of the Jordanian E-Government. *Journal of International Commercial Law & Technology* **6**(3) 151–164.

Antón, A. I., Earp, J. B., and Young, J. D. 2010. How Internet Users' Privacy Concerns Have Evolved Since 2002. *IEEE Security & Privacy* **8**(1) 21–27.

Ashrafi, N., and Kuilboer, J.-P. 2005. Online Privacy Policies: An Empirical Perspective on Self-Regulatory Practices. *Journal of Electronic Commerce in Organizations* **3**(4) 61–74.

Beldad, A. D., De Jong, M., and Steehouder, M. F. 2009. When the Bureaucrat Promises to Safeguard your Online Privacy: Dissecting the Contents of Privacy Statements on Dutch Municipal Websites. *Government Information Quarterly* **26**(4) 559–566.

Braun, V., and Clarke, V. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* **3**(2) 77–101.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. Understanding Emergence and Outcomes of Information Privacy Concerns: a Case of Facebook. *ICIS 2010 Proceedings*

Cai, X., Gantz, W., Schwartz, N., and Wang, X. 2003. Children's Website Adherence to the FTC's Online Privacy Protection Rule. *Journal of Applied Communication Research* **31**(4) 346–362.

Cha, J. 2011. Information Privacy: A Comprehensive Analysis of Information Request and Privacy Policies of Most-Visited Web Sites. *Asian Journal of Communication* **21**(6) 613–631.

Ciocchetti, C. A. 2007. E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. *American Business Law Journal* **44**(1) 55–126.

Clarke, R. 2006. A Pilot Study of the Effectiveness of Privacy Policy Statements. *BLED 2006 Proceedings*

Cottrill, C. D. 2011. Location Privacy: Who Protects?. *Journal of the Urban & Regional Information Systems Association* **23**(2) 49–59.

Culnan, M. J. 2000. Protecting Privacy Online: Is Self-Regulation Working?. *Journal of Public Policy & Marketing* **19**(1) 20–26.

Desai, M., Lodge, D., Gates, M., Wolvin, M., and Louer, G. 2012. The FTC Privacy Report: What the Report Means and how you can get Ahead of Enforcement Trends by Implementing Best Practices Now. *International Journal of Mobile Marketing* **7**(2) 26–36.

Earp, J. B., Antón, A. I., Aiman-Smith, L., and Stufflebeam, W. H. 2005. Examining Internet Privacy Policies Within the Context of User Privacy Values. *IEEE Transactions on Engineering Management* **52**(2) 227–237.

Faja, S., and Trimi, S. 2006. Influence of the Web Vendor's Interventions on Privacy-related Behaviors in e-Commerce. *Communications of the Association for Information Systems* **17**(1) 27.

Fang, Y. 2010. The Death of the Privacy Policy: Effective Privacy Disclosures after In Re Sears. *Berkeley Technology Law Journal* **25** 671–700.

Garrison, L., Hastak, M., Hogarth, J. M., Kleimann, S., and Levy, A. S. 2012. Designing Evidence-based Disclosures: A Case Study of Financial Privacy Notices. *Journal of Consumer Affairs* **46**(2) 204–234.

Hong, T., McLaughlin, M. L., Pryor, L., Beaudoin, C. E., and Grabowicz, P. 2005. Internet Privacy Practices of News Media and Implications for Online Journalism. *Journalism Studies* **6**(1) 15–28.

Hooper, A., Bunker, B., Rapson, A., Reynolds, A., and Vos, M. 2007. Evaluating Banking Websites Privacy Statements-A New Zealand Perspective on Ensuring Business Confidence. *PACIS 2007 Proceedings*

Hooper, T., and Evans, T. B. 2010. The Value Congruence of Social Networking Services-A New Zealand Assessment of Ethical Information Handling. *The Electronic Journal Information Systems Evaluation* **3**(2) 121–131.

Hooper, T., and Vos, M. 2009. Establishing Business Integrity in an Online Environment. *Online Information Review* **33**(2) 343–361.

Hossain, M. A., and Dwivedi, Y. K. 2014. What Improves Citizens' Privacy Perceptions Toward RFID Technology? A Cross-Country Investigation Using Mixed Method Approach. *International Journal of Information Management* **34**(6) 711–719.

Janson, H., and Olsson, U. 2001. A Measure of Agreement for Interval or Nominal Multivariate Observations. *Educational and Psychological Measurement* **61**(2) 277–289.

Kaupins, G. E., and Reed, D. 2012. New Media Usage and Privacy Policies of Newspaper Websites of the Baltic States. *Current Issues of Business & Law* **7**(1) 27–45.

Kim, S., and Yi, S.-H. 2010. Is Privacy at Risk when Commercial Websites Target Primary School Children? A Case Study in Korea. *Children & Society* **24**(6) 449–460.

Kubis, K. E. 2010. Google Books: Page by Page, Click by Click, Users Are Reading Away Privacy Rights. *Vanderbilt Journal of Entertainment & Technology Law* **13**(1) 217–254.

Kuzma, J. 2010. An Examination of Privacy Policies of US Government Senate Websites. *Electronic Government, an International Journal* **7**(3) 270–280.

Kuzma, J. 2011. Empirical Study of Privacy Issues among Social Networking Sites. *Journal of International Commercial Law and Technology* **6**(2) 74–85.

Landis, J. R., and Koch, G. G. 1977. The Measurement of Observer Agreement for Categorical Data. *Biometrics* **33**(1) 159–174.

Langenderfer, J., and Cook, D. L. 2004. Oh, What a Tangled Web we Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance. *Journal of Business Research* **57**(7) 734–747.

LaRose, R., and Rifon, N. 2006. Your Privacy is Assured - Of Being Disturbed: Websites With and Without Privacy Seals. *New Media & Society* **8**(6) 1009–1029.

Liu, C., and Arnett, K. P. 2002. Raising a Red Flag on Global WWW Privacy Policies. *The Journal of Computer Information Systems* **43**(1) 117–127.

Magi, T. J. 2010. A Content Analysis of Library Vendor Privacy Policies: Do They Meet Our Standards?. *College & Research Libraries* **71**(3) 254–272.

McGrath, L. 2011. Social Networking Privacy: Important or Not?. *Interdisciplinary Journal of Contemporary Research In Business* **3**(3) 22–28.

McRobb, S. 2006. Let's Agree to Differ: Varying Interpretations of Online Privacy Policies. *Journal of Information, Communication and Ethics in Society* **4**(4) 215 – 228.

McRobb, S., and Rogerson, S. 2004. Are they Really Listening?: An Investigation into Published Online Privacy Policies at the Beginning of the Third Millennium. *Information Technology & People* **17**(4) 442–461.

Meinert, D. B., Peterson, D. K., Criswell, J. R., and Crossland, M. D. 2006. Privacy Policy Statements and Consumer Willingness to Provide Personal Information. *Journal of Electronic Commerce in Organizations* **4**(1) 1–17.

Metzger, M. J. 2006. Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure. *Communication Research* **33**(3) 155–179.

Milne, G. R., and Culnan, M. J. 2002. Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys. *Information Society* **18**(5) 345–359.

Mundy, D. P. 2006. Customer Privacy on UK Healthcare Websites. *Medical Informatics and the Internet in Medicine* **31**(3) 175–193.

Noy, N. F., and McGuinness, D. L. 2001. *Ontology Development 101: A Guide to Creating Your First Ontology*

O'Connor, P. 2003. What Happens to my Information if I Make a Hotel Booking Online: An Analysis of On-Line Privacy Policy Use, Content and Compliance by the International Hotel Companies. *Journal of Services Research* **3**(2) 5 – 28.

Organisation for Economic Cooperation and Development. 1980. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* Recommendation by the Council of the OECD

Papacharissi, Z., and Fernback, J. 2005. Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements. *Journal of Broadcasting & Electronic Media* **49**(3) 259–281.

Peslak, A. R. 2005. Internet Privacy Policies: A Review and Survey of the Fortune 50. *Information Resources Management Journal* **18**(1) 29–41.

Pollach, I. 2006. Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. *Journal of Organizational and End User Computing* **18**(1) 23–49.

Pollach, I. 2007. What's Wrong With Online Privacy Policies?. *Communications of the ACM* **50**(9) 103–108.

Proctor, R. W., Ali, M. A., and Vu, K.-P. L. 2008. Examining Usability of Web Privacy Policies. *International Journal of Human-Computer Interaction* **24**(3) 307–328.

Rains, S. A., and Bosch, L. A. 2009. Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements. *Health Communication* **24**(5) 435–446.

Rizk, R., Gürses, S. F., and Günther, O. 2010. SNS and 3rd Party Applications Privacy Policies and their Construction of Privacy Concerns. *ECIS 2010 Proceedings*

Robles-Estrada, C., Vargas-Barraza, J. A., and Sepúlveda-Núñez, M. D. del C. 2006. Are Privacy Issues Important in Mexican Online Markets? An Empirical Investigation into Published Online Privacy Statements of Mexican Web Sites. *BLED 2006 Proceedings*

Savirimuthu, J. 2013. Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance. *International Review of Law, Computers & Technology* **27**(1-2) 161–186.

Schuele, K. 2005. Privacy Policy Statements on Municipal Websites. *Journal of Government Financial Management* **54**(2) 20–29.

Schwaig, K. S., Kane, G. C., and Storey, V. C. 2005. Privacy, Fair Information Practices and the Fortune 500: The Virtual Reality of Compliance. *ACM SIGMIS Database* **36**(1) 49–63.

Schwaig, K. S., Kane, G. C., and Storey, V. C. 2006. Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures?. *Information & Management* **43**(7) 805–820.

Shalhoub, Z. K. 2006. Content Analysis of Web Privacy Policies in the GCC Countries. *Information Systems Security* **15**(3) 36–45.

Stanaland, A. J. S., Lwin, M. O., and Leong, S. 2009. Providing Parents with Online Privacy Information: Approaches in the US and the UK. *Journal of Consumer Affairs* **43**(3) 474–494.

Stitilis, D., and Malinauskaite, I. 2013. Evaluation of Legal Data Protection Requirements in Cloud Services in the Context of Contractual Relations with End-Users. *Socialines Technologijos* **3**(2) 390–414.

Strickland, L. S., and Hunt, L. E. 2005. Technology, Security, and Individual Privacy: New Tools, new Rhreats, and new Public Perceptions. *Journal of the American Society for Information Science and Technology* **56**(3) 221–234.

Sturm, B., Schneider, S., and Sunyaev, A. 2015. Leave No Stone Unturned: Introducing a Revolutionary Meta-search Tool for Rigorous and Efficient Systematic Literature Searches. *Proceedings of the 23rd European Conference on Information Systems (ECIS 2015)*

Suominen, H. 2012. Towards an International Electronic Repository and Virtual Laboratory of Open Data and Open-Source Software for Telehealth Research: Comparison of International, Australian and Finnish Privacy Policies. *Studies in Health Technology and Informatics* **182** 153–160.

Tavani, H. T. 2007. Philosophical Theories of Privacy: Implications for and Adequate Online Privacy Policy. *Metaphilosophy* **38**(1) 1–22.

Timpson, S., and Troutman, M. 2009. The Importance of a Layered Privacy Policy on all Mobile Internet Sites and Mobile Marketing Campaigns. *International Journal of Mobile Marketing* **4**(1) 57–61.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research* **22**(2) 254–268.

Unruh, H. K., Bowen, D. J., Meischke, H., Bush, N., and Wooldridge, J. A. 2004. Women's Approaches to the Use of New Technology for Cancer Risk Information. *Women & Health* **40**(1) 59–78.

US Federal Department of Health Education and Welfare. 1973. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Chapter III. Safeguards for Privacy*

Weitzman, E. R., Cole, E., Kaci, L., and Mandl, K. D. 2011. Social but Safe? Quality and Safety of Diabetes-Related Online Social Networks. *Journal of the American Medical Informatics Association* **18**(3) 292–297.

Wijnholds, H. de B. an. M. W. L. 2001. Regulatory Issues for Global E-Tailers: Marketing Implications. *Academy of Marketing Science Review* **2001** 1.

Wu, K.-W., Huang, S. Y., Yen, D. C., and Popova, I. 2012. The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust. *Computers in Human Behavior* **28**(3) 889–897.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. J. 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems (JAIS)* **12**(12) Article 1.

Yee, G. O. ., and Korba, L. 2013. Personal Privacy Policies. *Computer and Information Security Handbook*, John R. Vacca (ed.), 773–792.

Zhang, X., Toru, S., and Kennedy, M. 2007. A Cross-Cultural Analysis of Privacy Notices of the Global 2000. *Journal of Information Privacy and Security* **3**(2) 18–36.