Privacy in Context: An Evaluation of Policy-based Approaches to Location Privacy Protection

Dr. Caitlin D. Cottrill (Corresponding Author), Lecturer
University of Aberdeen
School of Geosciences
Elphinstone Road
Aberdeen, Scotland, UK AB24 3UF
Phone: +44 (0)1224 273694
c.cottrill@abdn.ac.uk

Dr. Piyushimita "Vonu" Thakuriah, Halcrow Chair of Transportation
University of Glasgow
School of Social and Political Sciences
Adam Smith Building, Glasgow, G12 8RT, Scotland
Phone: +44 (0) 141 330 6090
Piyushimita.Thakuriah@glasgow.ac.uk

International Journal of Law and Information Technology 22 (2): 178–207. doi:10.1093/ijlit/eat014.

Abstract:
In this paper, we expand upon earlier analysis of location-service related privacy policies in the public and private sector. Our intent is to identify key privacy components in an effort to more clearly and consistently address the privacy expectations of the public through the protections provided them by service and product providers. Through use of content analysis, we aim to determine how understandable current privacy policies are to the average consumer, how comprehensively they address identified components of privacy, and how consistently privacy is treated in the location arena. It is hoped that this analysis will assist with the development of practical and comprehensive approaches to privacy preservation in the area of Intelligent Transportation Systems (ITS) and Location-based services (LBS).

Keywords: Privacy policies, location services, content analysis

1. Introduction

The rapid growth in location-based and mobile technologies has led to massive increases in the amount of individual location information being collected. Public organizations, such as transit agencies and departments of transportation, may have access to detailed location data from RFID-enabled transit cards or GPS-enabled electronic toll collection systems. Location-sensing smartphone-based applications, such as Foursquare, Loopt and Twitter, have the ability to collect detailed information on a person's whereabouts and combine this information with a unique device identifier, contact information, and even a user's social network. According to the Wall Street Journal (2010), "An examination of 101 popular smartphone 'apps'—games and other software applications for iPhone and Android phones—showed that 56 transmitted the phone's unique device ID to other companies without users' awareness or consent. Forty-seven apps transmitted the phone's location in some way. Five sent age, gender and other personal details to outsiders." Findings such as these, combined with the increasing ubiquity of smartphones, have led to a wide range of discussions and debates around the notion of location and mobile privacy.

According to Liu (2009), "From the privacy policy perspective, location privacy refers to the claim (right) of individuals, groups, and institutions to determine for themselves, when, how and to what extent location information about them can be communicated to others." In this context, "privacy policies" that are available in websites or with mobile apps are defined as legal documents that disclose a web site or a service's practices regarding the ways in which the site or service gathers, uses, discloses, and/or manages a user's data or information generated by users. These are available either as stand-alone documents or within Terms of Agreements of websites and apps.

Worldwide, new policies and procedures related to the privacy of mobile and location data are beginning to emerge, with the EU Data Protection Working Party adopting an Opinion on Geolocation services on smart mobile devices in May of 2011, and the US Congress and Senate both holding hearings related to location based services and privacy in 2011. In addition, Google's recent privacy policy changes, including those related to location and mobile data, have seen a flurry of responses, including from the Office of the Canadian Privacy Commissioner (McKay, 2012), a collection of US Attorneys General (National Association of Attorneys General, 2012), and a collection of Privacy Commissioners from the Asia Pacific region (including New Zealand, Australia, Canada, Mexico, Hong Kong and South Korea (Sydney Morning Herald, 2012)).

These findings and activities underscore the importance of privacy policies in the landscape of mobile and location services, and indicate the growing recognition that effectively managing and communicating their related practices will be a key point of future use. From this recognition, however, emerge three related questions: first, how effective are current mobile and location-based privacy policies at communicating practices to consumers; second, how comprehensive are these polices; and third, is there consistency in how location and mobile data are treated across a range of service providers. The answers to these questions will have far-reaching ramifications for both the manner in which location privacy is treated from the point of view of local and national governments as well as for the understanding of privacy from the point of view of the consumer.

This paper will attempt to address these questions by reviewing the privacy policies of 101 public and private organizations that offer location and mobility services as a part of their Intelligent Transportation Systems (ITS) and Location-Based Services (LBS) programs. Based on an analysis of

these policies, we aim to determine, first, how understandable they are to the average user, second, how comprehensively they address different components of privacy, and, third, how consistently privacy is treated across these policies. A similar approach was taken in Cottrill and Thakuriah (2011); however, that evaluation was limited to an analysis of privacy policies of private companies, and based primarily on frequencies of words relating to locational privacy and by the presence or absence of elements of privacy concern such as notice, consent, redress policies and so on (as defined in Section 2.1 below). Here, we expand upon that research, first, to include a wider range of organizations in order to better understand how privacy is treated within both public and private contexts. Next, we use content analysis to broaden the analysis to look more deeply at clustering and correspondence within and between policies in order to provide more detailed information on how policies differ, and how included privacy elements may relate to one another. Our aim is to expand the growing literature on location privacy in the transportation realm by providing a more comprehensive approach to ascertaining how privacy is addressed by organizations and presented to the consumer.

The results of this analysis will be used to identify key components in efforts to move towards more unified and effective location privacy policies that reflect the needs of consumers, governments, and service providers. Of note is that, while the analysis will focus on the privacy policies of US-based firms and organizations, the overall findings from the analysis are applicable across a wide range of services and locations, particularly as applications and services developed in one nation or state may easily be transported across borders. Additionally, the approach used is one that is generalizable to other policy evaluation activities, thus developing a prototype approach by which other analysis may take place.

2. Background

Studies of location privacy tend to be grounded in either a technological or a policy-based methodology. While some approaches work to balance the overlapping needs of the two, it is rare that consumer needs and desires are reviewed in the context of applications of technology or the policies that guide them. There is an extensive literature available on technological approaches to protection of location privacy (see, for example, Ardagna, et al., 2011; Xu, et al., 2010; Ban and Gruteser, 2010; Liu, 2009); however, many of these studies have been undertaken as general reviews of how location data may be protected in the absence of an understanding of those data that users of location services may find most sensitive. Policy reviews may, on the other hand, take place in the absence of understanding of the potential for privacy violations in terms of data collection and availability in the presence of location technologies. The gap between the two may be addressed by either evaluating the willingness of consumers to trade privacy for location services, or by evaluating policies in the context of the user's expectation of privacy.

Potoglou, et al. (2009) have provided perhaps the clearest example of how the first of such studies may take place, in their approach to evaluation of the willingness of persons to make trade-offs between privacy, liberty and security. In this study, the authors note that, "While research on the security of public transport systems has been extensive from a public spending and benefits perspective, individuals' preferences have hardly been explored…" (Potoglou, et al., 2009) In their exploration of these preferences, the authors use a stated preference approach to evaluate and quantify the willingness of persons to trade privacy and liberty for a safer and more secure travel

experience on public rail in the UK. By using this approach, combined with evaluations of consumer trust, the authors were able to test various scenarios that provide insight on how users may value actions taken to protect their security within the context of their privacy preferences and beliefs, thus providing an examination of the "gap" between public policy and user preference.

This gap between policy and preference highlights the importance of trust in respect to privacy issues, particularly as it takes place, like travel, in the public realm. Privacy policies in location services hinge on the relationship of public expectations, legality and trust. While it is critical from the point of view of service providers to ensure that their privacy policies address privacy issues as required by applicable laws and regulations, it is also important that they (either solely by their existence or by their contents) convey a sense of trust to the user, such that they will provide an incentive for use of the application or service. Relationships between data producers, collectors, and consumers are based on a number of factors, including the degree to which data producers trust that the collectors and consumers will respect the contextual norms associated with these data. The relationship between trust and privacy has been examined by a number of researchers, including Karvonen (2010), Liu, et al. (2004), and Metzger (2004). Generally, it is found that the concepts of privacy and trust are closely linked, with trust serving as an intermediate variable in consumer willingness to release private information to agencies and organizations (Liu, et al. (2004)).

In the context of ubiquitous computing ("ubicomp") in the mobile environment, Karvonen (2010) states the following, "Ubiquitous systems gather information from their users and the user has to be able to trust the system to give out the needed information regarding him/her. Furthermore, the ideology of invisibility with ubicomp systems causes extra requirements for the development of user acceptance and trust." Ubiquitous computing in the mobile environment, whether in the form of current technologies such as location-based applications and GPS-enabled mobile technologies, or of proposed technologies such as peer-to-peer safety information, may be largely invisible to those using the system, thus requiring both enhanced consumer data protection, as well as fairly transparent implementation.

Recent privacy-related violations from such companies as Facebook (Helft, 2010), Apple (Zyskowski, 2011), and Google (Halliday, 2010) have put privacy concerns at the forefront of policy and technology issues as they relate to location-enabled technologies. Such a trend is clearly evident in findings from a recent survey conducted by Harris Polls for TRUSTe (2011) which showed that, "Privacy concerns rank #1: Most consumers expressed great concern about their data privacy both when using smartphones in general, and when using mobile apps in particular..." Given that companies generally limit communication of their privacy preservation methods to privacy policies (whether stand-alone or embedded in terms of service), ensuring adequacy of these policies is necessary to assure the user, and protect the rights and responsibilities of both the user and the agency of interest. Negative publicity or general distrust in government agencies or private corporations may enhance privacy concerns in the absence of adequate policies, and erode the trust necessary to help enhance likelihood of technology adoption on the part of consumers. Carefully constructed, readable, and comprehensive privacy policies and statements may be useful here, as indicated by Hui, et al. (2006); however, there are few available metrics for evaluating how well current privacy policies reflect categories of interest within the domain of locational privacy. The next section will first identify one method of approaching these categories, followed by an initial description of the policies of interest.

The most common privacy metric currently in use is that of Fair Information Practice Principles (FIPPs) (Shapiro (2012); Hansen, *et al.* (2008); Shilton (2009)). First introduced in 1973 by the HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems, The Code of Fair Information Practices evolved over time to become the basis for FIPPs, as outlined by the US Federal Trade Commission (FTC, 2007), which identifies the following components as needed to provide adequate safeguards for privacy protection:

- Notice/Awareness: The basis for privacy protection; notice should be given to consumers before any personal information is collected in order for them to have the foundation for making an informed choice about whether or not to share.
- Choice/Consent: Provision of an option for consumers regarding whether or not to share private data and for what it may be used.
- Access/Participation: The ability of a consumer to access data that has been collected on him or her and correct, amend, or have removed that data if it is incorrect.
- Integrity/Security: The need for data collectors to ensure that their data is stored and managed securely, both through technological and administrative means.
- Enforcement/Redress: Provision of a mechanism for enforcement of the above principles.

These principles are reflected to varying degrees in the privacy policies of several umbrella organizations with ties to the location services and ITS industries, including ITS America, CTIA – The Wireless Association, and VII/IntelliDrive (Cottrill and Thakuriah, 2011); this, along with their standardization and comprehensiveness, has led to them being chosen as the basis upon which policy analysis will take place. Here, we are to some point constrained by current privacy preserving practices. While the FTC criteria are generally adequate for determining overall privacy dimensions, there may be issues that arise with the introduction of location's spatio-temporal attributes. While the above categories capture the essence of needed privacy information, there may be need for more explicit directions to be given pertaining to how different types of data should be addressed for privacy protection. For purposes of this analysis, however, we will retain the FTC criteria in order to work within the prevailing paradigm.

As noted in the introduction, we focus here primarily on the US case; however, it should be noted that the issues, concerns, and constraints we address reach far beyond the borders of the United States. As noted in Cottrill (2011), location data and spatial services are generally not limited by geographic boundaries. While distinctions can be made in concerns relevant to spatially-bounded services (such as electronic toll collection media) and those that function worldwide (such as Foursquare), the fundamental components of privacy outlined in the FTC FIPPs are generally applicable to privacy and data protection regulations and directives from a wide variety of countries, and issues in their communication are of general concern to both public and private agencies and organizations worldwide (Cottrill, 2011). In this analysis, we hope to provide a review that, while bounded geographically in scope, may add to the wider literature on methods and recommendations for privacy protection applications in a spatially unbounded perspective.

3. Data and Research Approach

As described earlier, the primary approach to determine whether privacy policies may be instruments to safeguard the privacy of the user's location information is to examine a sample of

existing policies. We then evaluate, using the criteria presented in the previous section and content analysis, the extent to which the policies address privacy concerns. In the following subsections, we present the data collection method used and the analysis approach.

3.1 Sampling, Policy Selection and Data

Due to the rapid emergence of LBS applications and services, as well as increasing adoption of ITS technologies by public agencies, policies selected for analysis represent a convenience sample of all possible policies. This is because we do not currently have a complete sampling frame from which to randomly select policies, as the universe of organizations which offer location-based services, and the myriad services which these organizations offer, is not known. While we have attempted to construct a sampling frame from established sources (such as Directions magazine as described below), we believe that these sources will under-represent smaller companies supplying mobile location-based services (for example, the one-person app developer or non-profit organization). We have stratified organizations which provide mobile location and transportation services into private service providers, public service providers, Electronic Toll Collection agencies and Electronic Transit Fare collection agencies. It should be noted that these distinctions have been made primarily for purposes of analysis, as consumers often do not differentiate between the type of organization providing a service and/or collecting data. For our purposes, however, underlying distinctions in legal and/or regulatory requirements for public versus private organisations indicate the need for a more differentiated study. Table 1 below provides a general overview of the organization types selected for evaluation and examples of services they provide. The organization types and the methods used to select them will be described in more detail below.

Table 1: Agency Types of Policies Evaluated

Type of Organization	Sample Size	Examples of Services Provided
Private ITS or LBS Service Provider	48	Navigation services Social networking Mobile commerce Entertainment and service guides Traffic information
Public Service Provider	34	Transit information and navigation Traffic information Public services
Electronic Toll Collection (ETC)	7	Provide electronic toll collection services and associated devices
Electronic Transit Fare (ETF)	12	Provide services for electronic payment of transit fares

Public service providers include both transit providers and public Departments of Transportation (DOTs) that may be affiliated with transit providers or that host the privacy policy for transit providers. To select privacy policies of these public agencies, the Federal Transit Administration's website was first used to identify the universe of transit or transit-related agencies. These agencies

were then assessed to determine if (a) they provided privacy policies, and (b) if they currently use electronic transit (or fare) (ETF) cards. If they currently provide ETF or ETC services, they were split into a separate category, described below. For the remaining agencies, if a privacy policy was provided, it was retained for analysis.

Privacy policies related to ETF services, though often aligned with public service providers and guided by overarching policies applicable to the relevant DOTs or city or state governments, were analysed within a separate category. This decision was made based on an initial, cursory analysis that revealed substantial differences in the contents of the two policy types. Such differences include, for example, the addition of detail related to financial considerations and associated extensive personally identifying information. An additional consideration was that overarching privacy policies for agencies that provide services such as trip-planning targeted at transit service users are generally accessible from a number of platforms (such as on paper, on a service website, or via mobile phones), while those geared for ETF (and ETC) use are generally included in terms of service or application agreements, which may be accessed only at the point of application. Because of these differences, ETF policies have been analyzed separately from overall public service policies.

For electronic toll collection (ETC) policies, a web search was conducted to identify currently implemented ETC systems in the United States. Of the ETC systems identified, seven had publicly available privacy policies, which were gathered and pre-processed. Additional ETC providers were contacted in an attempt to obtain additional privacy policies; however, no additional policies were received. As with ETF policies, some ETC networks are administered through public agencies; however, due to the differences in content in these policies when contrasted with general public agency policies, they were analysed in a separate category.

A directory of LBS companies available from Directions Magazine (2010) was used to identify specific private mobility information companies, from which a total of 48 companies were retained. A majority of the companies are headquartered in the U.S, and all operate within the U.S. While the Directions Magazine listings may not be a fully accurate sampling frame of the universe of such companies operating within the U.S., it does provide a fairly comprehensive overview of companies of interest. As with public services, there are a large number of private ITS and LBS agency types, serving both individuals and manufacturers of services targeted at individuals (such as provision of background maps for mobile navigation systems). While the privacy policies of these agencies may have differing impacts on the individual at the personal level, the ability of such service providers to collect both primary and secondary data (as third-parties to other services) makes the applicability of these policies to individuals in the locational environment of equal worth. Because many of the agencies that partner with other agencies to provide enhanced mobile services for consumers may have access to data collected by partnering agencies, the privacy policies of these agencies are relevant to consumer privacy concerns. Here, as with general public agency policies described above, policies tend to be accessible online or per use, as opposed to being overtly stated primarily at time of initial application. Thus, the characteristics of policies of all agency types have been treated as broadly similar for purposes of the analysis.

3.2 Methodology to Analyse Privacy Policies

The analysis of privacy policies was designed to respond to the overarching question of, “To what extent and by what methods should privacy in ITS and LBS be protected”. Privacy policies were

chosen as the units of analysis here, as these are the primary methods by which agencies and organizations inform consumers as to how their personal data will be collected, stored, managed, shared and protected. Because there is no overarching privacy policy relevant to location data currently in place, the Federal Trade Commission's Fair Information and Privacy Principles were used to develop baseline categories of interest, as described below. In this section, we provide an overview of the methodological approach to analyze privacy policies.

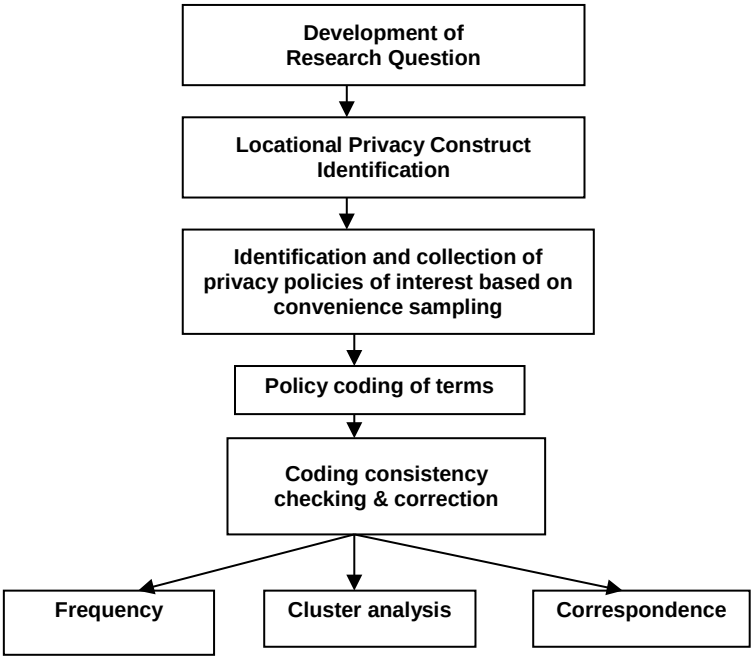
We evaluate the privacy policies using several criteria. First, we determine the extent to which a privacy policy specifically addresses the data and location information aspect of the mobility service. Second, we address the extent to which the policy may be easily understood by a typical user by using a readability score. Third, we use content analysis as a way to systematically analyze the text in the privacy policies and to determine the extent to which the policies address privacy by using metrics connoted by the FTC FIPPs. For the content analysis, we make use of word frequencies to examine the extent to which the metrics are present in the policies and cluster analysis to identify which groupings of criteria may be more closely aligned with one another contextually.

As described previously, we began by selecting a sample of privacy policies that became the set of items that were subject to a content analysis. Content analysis is used here to evaluate, first, differences in the treatment of privacy notifications to consumers by public and private agencies and, second, to identify gaps in the information presented to consumers on the treatment and use of their travel data. In general, content analysis enables an objective description of the manifest or written content of textual material (Berelson, 1974), by determining the presence of themes, phrases or other related attributes of the material (Nuendorf, 2002). Once the set of texts to be analyzed were identified, we next broke them down into component units of analysis, in this case words and phrases, that were then coded into constructs of interest.

Subjectivity has been noted to be of concern in content analysis and Kassarjian (1977) stated that reproducibility of results by different analysts analyzing the same content is a key requirement of objectivity. For purposes of this research, the issue of subjectivity has been addressed, in part, via the use of the automated content analysis software WordStat. It should be noted, however, that a text will always involve multiple meanings and that there is always some degree of interpretation required on the part of the researcher (Graneheim and Lundman, 2004). Quantitative content analysis bypasses this difficulty to some degree by holding to the rigors of statistical analysis requirements, but it is difficult to argue that any content analysis will be completely free from the biases of the researcher and text coder.

For this analysis, the constructs of interest were developed and operationalized into metrics by reviewing the constructs and questions of interest in relation to the current treatment of privacy in regard to law and legal issues. These steps required identification of a broad underlying set of categories of interest in relation to privacy, for which the FTC's categories identified above were chosen. Policies were collected, coded and tested for consistency before performing the detailed statistical analysis. Figure 1 provides an overall description of the steps undertaken.

Figure 1: Content Analysis Process Flowchart



Both cluster and correspondence analysis are used for purposes of the content analysis. For the cluster analysis, the main objective is to split the set of privacy policies according to some textual feature variables, in this case constructs of interest from the FTC as described above. From this splitting, the similarity of entities is assessed based upon the comparisons of attributes they contain. For the computational step in determining similarity, many measures have been suggested including correlation coefficiants, distance measures, association coefficients and probabilistic similarity measures (a far from complete list referring to this voluminous literature includes Al Khalifa, et al, 2009; Sneath and Sokal, 1973).

We used Euclidean distance to determine similarity, where distance is calculated based on user-defined "cases" (here defined as policies of interest), and then compared to other cases to determine similarity. This type of method may be generally called an agglomerative hierarchical clustering method, as it begins with many individual elements which are successively combined based on distance measures until only one cluster remains, containing all elements of interest. We have used dendrograms to visually display the results of the hierarchical clustering structure. Additional graphical analysis, using correspondence analysis, was utilized in order to observe interrelationships between terms identified from the privacy policies and privacy metrics derived from the FTC criteria, in 2- or 3-dimensional space. This visual tool allows us to identify and describe how well policies of interest respond to constructs and categories of privacy interest identified in the FTC policy, as well as to examine if there are patterns in how these constructs are treated by different types of agencies or organizations.

4. Description of Privacy Policies

In terms of the *specificity* of the content of the policies, privacy policies evaluated here fall into two general categories: first are those that deal generally with privacy issues over a range of services offered by the organization (such as website, mobility services, and applications); second are those that specifically address the privacy issues inherent in use of a mobile service or application. The distinction here is an important one, as data gathered from each of these sources will provide varying degrees of personal information related to a traveler's location, preferences, and patterns of use. In collecting privacy policies for this analysis, efforts were made to concentrate on specific polices related to the use of applications and services offered by providers; however, in many cases available policies were generic and related to general data collection policies and website use.

While all of the policies of private providers referred to use of their websites, only a few referred specifically to how the privacy policy will be implemented with respect to products, services or location information. Roughly 49% addressed the specific product or service, while 42% addressed location-specific information. This finding was concerning, as it reflects that many companies do not recognize and/or acknowledge that privacy concerns specific to location information may exist. General privacy policies of public service providers are not linked to specific applications, and thus generally do not address location- or product-specific information. As noted above, those providers that do provide services that may be able to track location data (such as ETC or electronic transit cards) have had their policies evaluated separately.

In terms of the ability of users to *comprehend* the policies, as noted in our earlier paper, the Office of Educational Research and Improvement (2002), estimates that the average reading level of U.S. adults is between the 8th and 9th grade. The Flesch-Kincaid Grade Level calculator, which uses average sentence length and average number of syllables per word along with weighting factors to determine a reading level, is a standard test used to ascertain the general readability of texts as measured by US grade level. The test was applied to each policy considered, resulting in the following averages:

- Overall average (all companies): 14.60 (range of 9.71 – 24.50)
- Overall average (public organizations): 14.33 (range of 11.43 – 19.02)
- Overall average (private companies): 14.27 (range of 9.71 – 24.50)
- Overall average (ETC providers): 13.87 (range of 10.09 – 17.69)
- Overall average (Electronic Transit Card providers): 15.34 (range of 12.09 – 23.06)

These figures indicate that the overall average reading grade of the privacy policies studied here is roughly that of a sophomore to a junior in college, well over that of the average US adult. Such a finding provides a baseline indication that the privacy policies used by mobile transportation service providers may not be understandable by the average user, and thus do not meet the FTC's general notice provision.

4.1 Categorization

Categorization allows for individual words or phrases to be grouped under a common heading, thus simplifying the process of analyzing text within headings of interest. As noted above, the metrics operationalizing the FTC's five FIPPs categories were used for this purpose here. Words and phrases within the identified privacy principles were assigned to a category based upon their most common uses and meanings. To effectively categorize words, a number of policies were reviewed to determine how words and associated phrases were used within the context of the policies. Words and phrases within policies were next assigned a category and then these categorizations were compared across policies to ensure consistency.

Once words and phrases contained in the document were categorized and subjected to the consistency check, a frequency analysis was run at the category level to determine how often policies referred to the assigned topics. While some words tended to overlap in different categories, most were able to be effectively and accurately classified into overall categories. Table 2 outlines how frequently occurring words were categorized. Two separate analyses were performed: one on privacy policies of public companies and one of privacy policies of private companies. The next section reviews results of each of the two analyses. Here, we build upon results from Cottrill and Thakuriah (2011) but expand to provide more detailed analysis and to allow for a comparison between public and private organizations. This addition broadens both the scope and applicability of the project.

Table 2: Privacy Policy Word Categorization

Content Analysis Database Keyword Categorization					
Classification	**Privacy Concept Category**	**Keywords**	**Classification**	**Privacy Concept Category**	**Keywords**
Access/ Participation	Contest Change	Contest	**Notification/ Awareness**	About	Assurance
		Incorrect			Changes
	View	View			Children's Privacy
	Choice/Consent	Opt-in		Collected Data	Address
		Opt-Out			Birthdate
Enforcement/ Redress	Contact	Contact			Device
		Questions			Device ID
	Government Enforcement	Government			IP Address
		Legal Claims			Location
		Legal rights			Password
		Required by law			Personal Information
		Safe Harbor			Phone number
		TrustE			Name
	Private Remedies	Disclosure			Preferences
		Fraud			Username
		Illegal			Zip code
		Investigate		Cookie use	Cookie
		Prevent		Cookies and Clickthrough	Beacon
		Take action		Data Mining	Combine
		Transfer			Mine
		Violation		Data Use	Advertising
		Terms of use			Billing
	Self Regulation	Your responsibility			Contests
		You guard			Outreach
		Protect your			Publicity
Integrity/ Security	Managerial	Managerial			Support
		Administrative			User experience
		Procedural		Ownership	Ownership
	Technical	Electronic			Own
		Technical		Third Parties	Advertisers
		Physical			External links
		Protect			Government agencies
		Security			Partners
					Third parties
					Vendors
				User Action	Check in
					Download
					Make a call
					Report location
					Send a text message
					You send
					You tell us
					You click

4.2 Frequency Analysis

A general frequency analysis was conducted in order to describe the landscape of the presence of identified privacy elements in the privacy policies of both public and private providers, as well as policies associated with ETC and electronic transit card services, as shown in Figures 2 and 3, which demonstrate, first, the relative occurrence of keywords in specific categories compared to those of other categories, and, second, how often the criteria metrics were present in the policy category of interest. Clear differences and similarities in the topics addressed by policies in each category quickly emerge. Overall, it is evident that the "Collected Data" category is the most widely addressed, with elements cited by roughly 97% and 98% of public and private companies, respectively. Such a finding is unsurprising for a number of reasons: 1) the number of words included in this category (13) is higher than that of any other category, and 2) The overarching category ("Notification/Awareness") is often considered the fundamental privacy principle, as it is notification of rights and

responsibilities that encourages the development of privacy policies. This finding is not accurate , however, for ETC and transit card providers, with only 14.4% of these policies addressing this issue. This finding may be related to these policies addressing only general confidentiality practices, and relying on agency privacy policies for more substantive information.

Private companies were generally likely to address more aspects of privacy as identified in the FTC guidance, with some exceptions such as Children's Privacy, language referring to notification of changes to the privacy policy, and actions related to third parties. Public agencies, on the other hand, fall short in their addressing of managerial means of privacy protection and the issue of how users may contest or change collected data. ETC and electronic transit card providers, in general, demonstrated overall inconsistency with policy framing when compared to both public and private policies. This may, again, be related to reliance on general privacy policies to address more specific areas of privacy (such as children's privacy or data collection and use policies), but may also reflect a difference in how privacy terms for these policies differ significantly from those of more comprehensive service providers.

Figure 2: Percentage Frequencies of Category Metrics within Coded Criteria

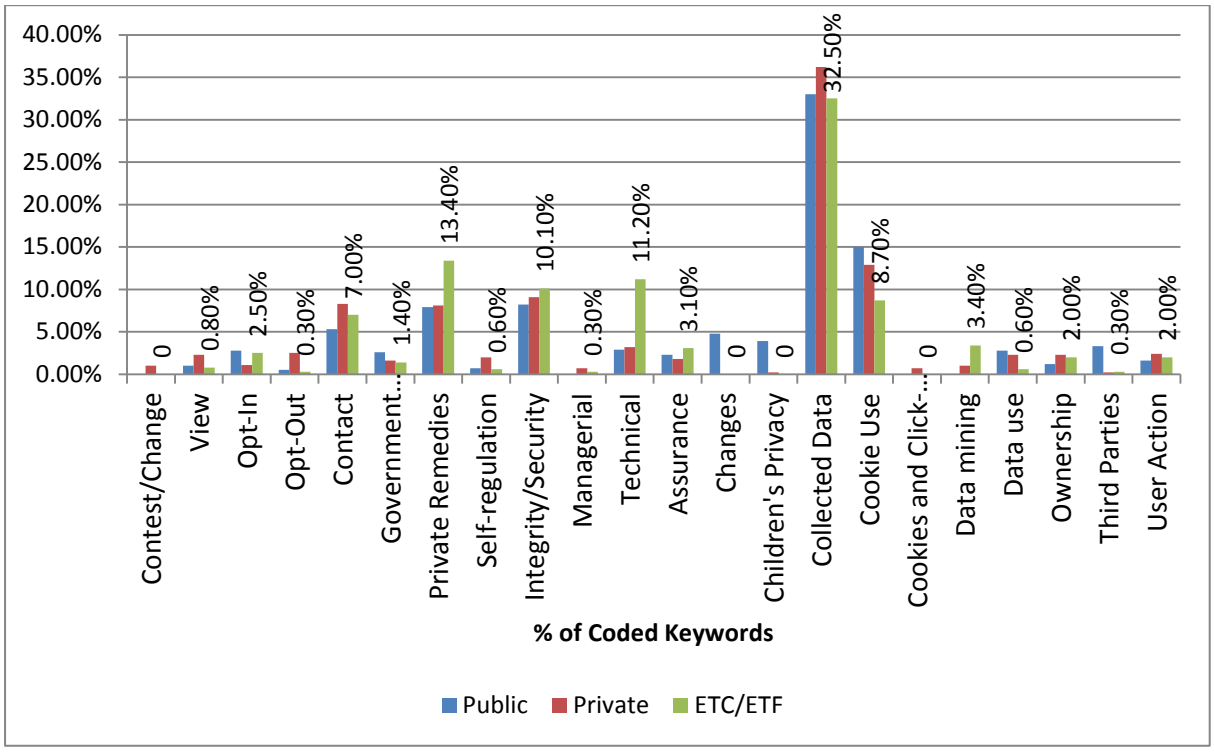
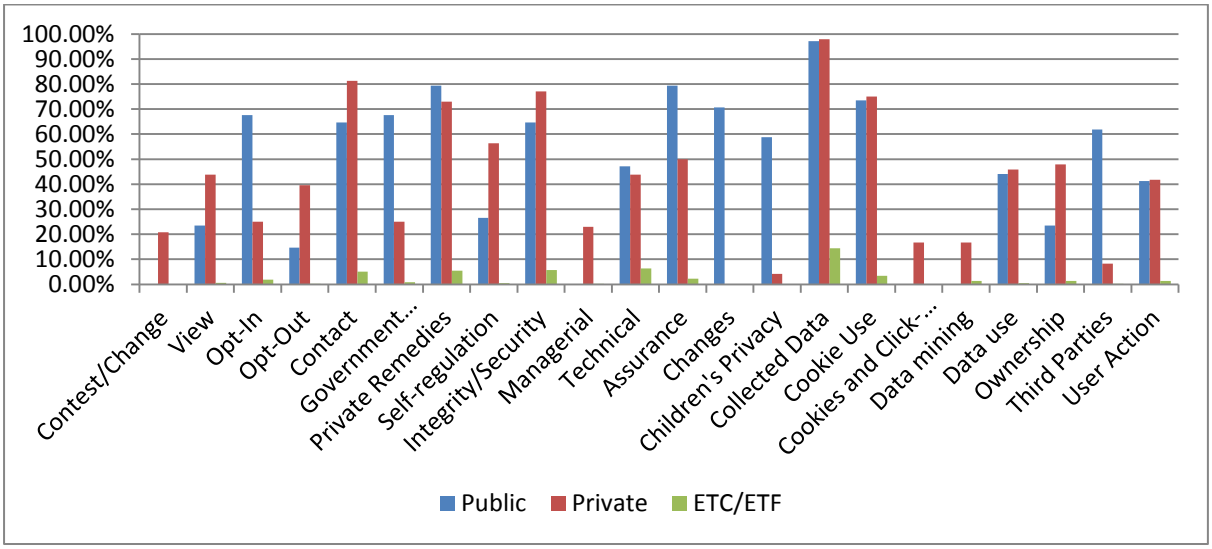


Figure 3: Percentage of Policies Referencing Specific Category Topics



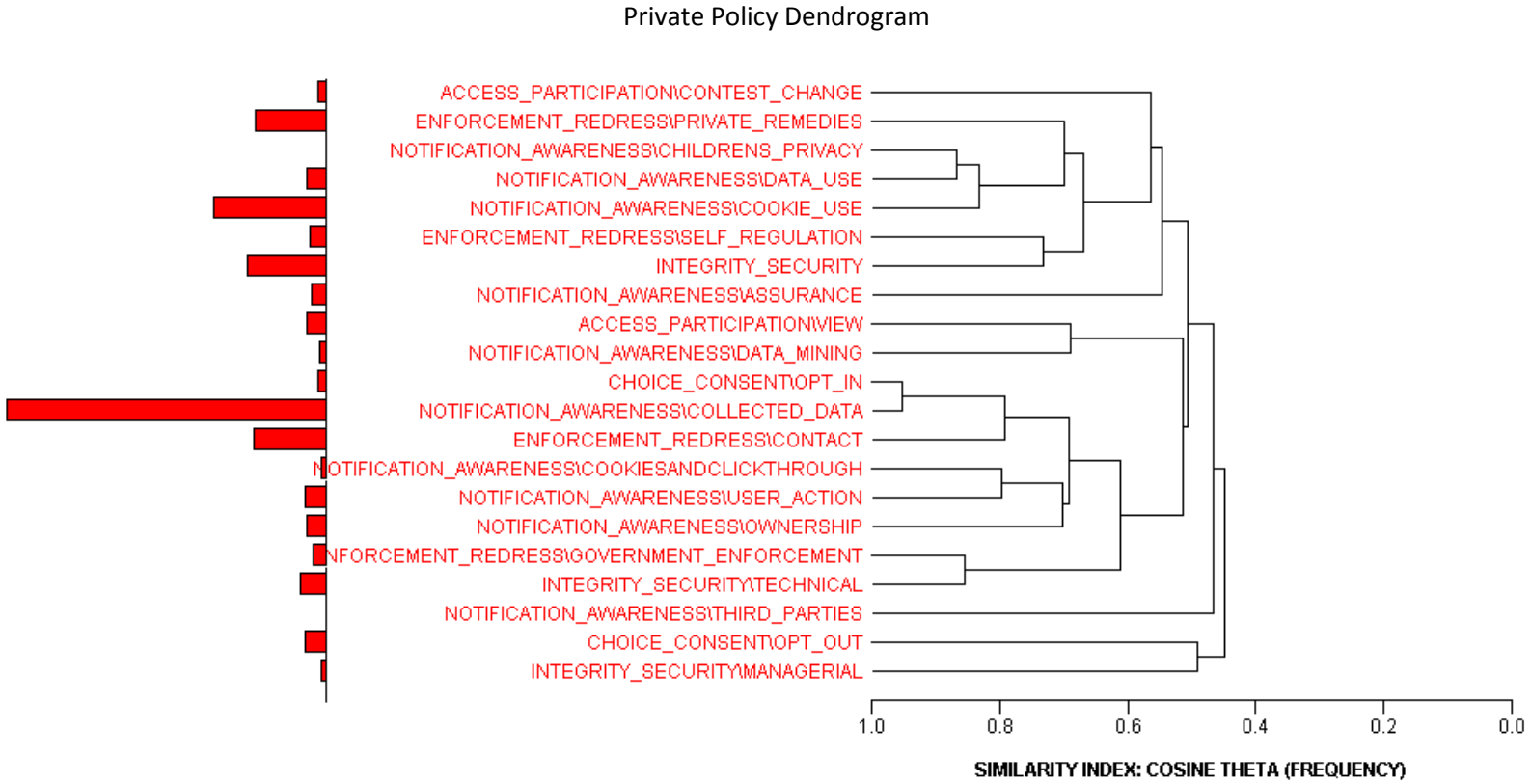
Frequency analysis, on its own, is insufficient to evaluate the overarching comprehensiveness of privacy policies, as it does not allow for the context of identified elements to be adequately described. For example, while it is of use to determine how many organizations or agencies refer to either "Self-regulation" or "Contact" under Enforcement/Redress, it may be of more value to ascertain how many policies refer to both concepts, and to what extent the two are related, in order to determine the degree of input the consumer has on protection of his or her privacy. In order to evaluate such measures, cluster analysis may provide additional insights.

4.3 Cluster Analysis

Figure 4 shows a dendrogram which visually depicts the results of the cluster analysis. In a dendrogram, the vertical axis is made up of the items and the horizontal axis represents the clusters formed at each step of the clustering procedure. Words or categories that tend to appear together are combined at an early stage while those that are independent from one another or those that do not appear together tend to be combined at the end of the agglomeration process (Provalis, 2010).

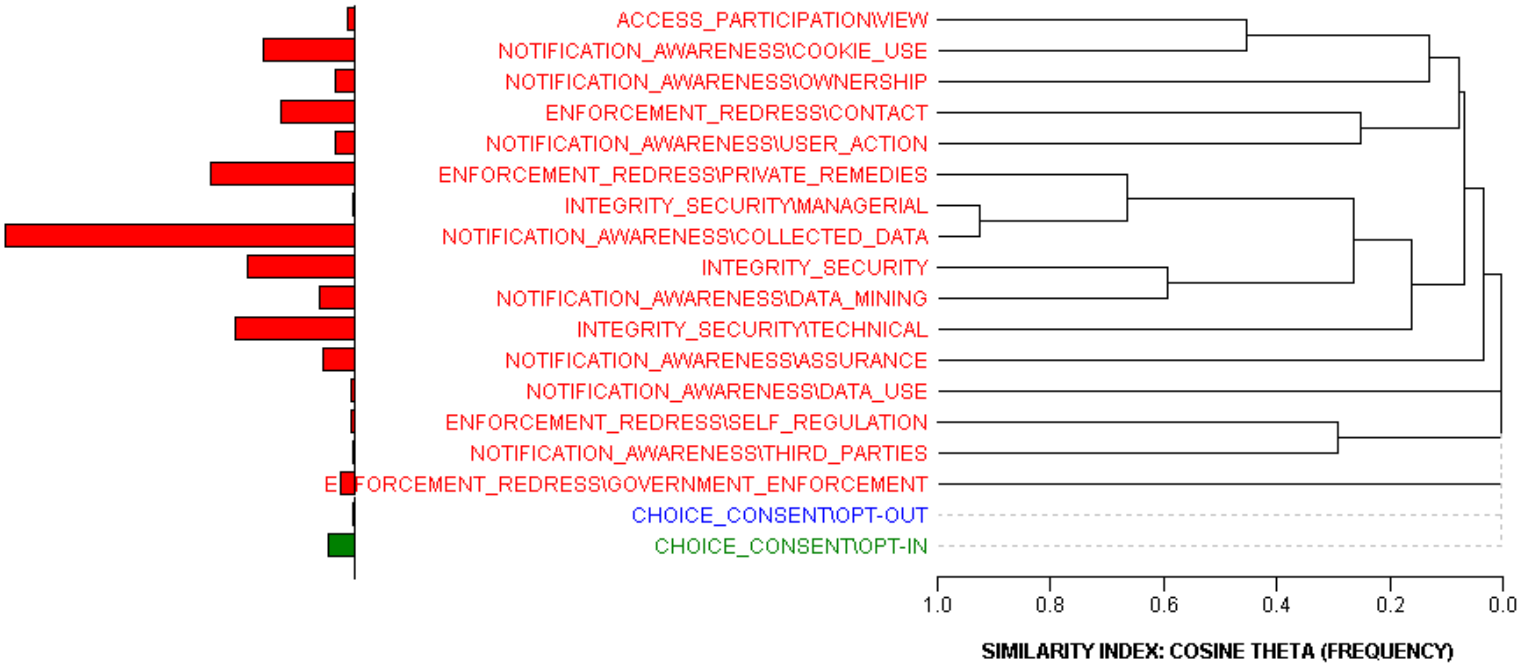
For purposes of this analysis, we have chosen to use cosine theta, which, "…measures the cosine of the angle between two vectors of values. It ranges from -1 to +1" (Provalis Research, 2010). This method has been chosen as it takes into account not only the presence of a word or phrase in a case, but also how often the word or phrase occurs. This additional information will allow for better determinations of similarity to take place. Dendrograms using cosine theta for private and public privacy policies, as well as ETC and electronic transit card policies are shown in Figure 4.

Figure 4: Policy analysis dendrograms identifying clusters of related concepts



Public Policy Dendrogram

ETC and Electronic Transit Card Dendrogram



From the dendrograms above, we can determine weight, compactness, and distinctness, which are defined as follows:

- Weight - the rough percentage of all individuals that fall within each cluster
- Compactness - how similar to one another the elements of a cluster are
- Distinctness - how different one cluster is from its closest neighbor (ESRI, 2002)

From the dendrograms above, one can see that public and private privacy policies and ETC/Electronic Transit Card policies have quite different structures regarding the presence of various privacy metrics. For example, for private policies the codes for "Opt-in" and "Collected data" are quite compact, indicating that they are fairly similar in presence. The weight of the primary cluster which contains these elements is also fairly high, with 38% (eight of 21) of criteria elements falling within this cluster with a similarity index of 0.6. Such a finding indicates that the clustered elements (Opt-in, Collected data, Contact, Cookies and Click-through, User action, Ownership, Government enforcement and Technical) are relatively similar in their presence within the privacy policies of the included private agencies. While at first glance the cluster may seem odd, it is clear that each of the included elements are, a) seen with relatively high frequency according to Figure 3, and b) primarily related to Notification/Awareness. The clustering of these concepts indicates that they are closely related within the objectives of these privacy policies within the private sector.

A second fairly compact cluster consists of the following six elements: Private remedies, Children's privacy, Data use, Cookie use, Self-regulation and Integrity/security. While still primarily concerned with Notification/awareness, this cluster is more closely concerned with how consumer data are used and protected. The relatively higher inclusion of Enforcement/redress categories here indicates that those companies that include some information regarding the protection of consumer data are also likely to include information on the uses of those data. It is possible that the relative freedom of private companies as opposed to public companies to determine enforcement mechanisms may play a role in this clustering.

For public provider privacy policies, the landscape is somewhat different. The closest cluster in this area is that of Assurance and Ownership, both included under Notification/awareness. The Assurance element is a somewhat general category, consisting primarily of statements related to general assurances of privacy for the consumer (such as, "Agency X values your privacy", etc.). Such assurances are fairly generic, thus their close association with the element of Ownership, which occurs in a relatively small number of cases, is somewhat surprising. In all, based on the clusters identified, there is less overall consistency of content in public privacy policies than in their private company counterparts; however, as with private companies, one fairly large cluster does exist. The largest and most compact cluster is composed of the following elements: Government enforcement, Technical, Data use, Changes, Children's privacy, Third parties, Assurance, Ownership, and Cookie use. As above, this cluster has a similarity index of 0.6, indicating fairly close association. As with the private company policies, Notification/awareness is the primary category associated with this cluster; however, the types of information provided to the consumer is somewhat different. One possible rationale for this is that such elements as the protection of children's privacy are mandated under federal law, and are thus more likely to be included by government agencies. Also, more strict regulations regarding the sharing of data by public agencies may make more explicit information regarding this element more common. In general, however, it appears that like elements tend to be

clustered with like, indicating that there are some limitations as to the comprehensiveness of policies in addressing each of the above-identified primary categories.

Clusters seen in ETC and electronic transit card policies are markedly different from those of both public and private service providers. Here, the closest cluster is that of "Managerial" and "Collected Data," with a similarity index of roughly 0.9, indicating that these two concepts are closely related in these policies. Such a close relationship reflects, in part, the reliance upon the concept of "data confidentiality" in these agreements, with many policies indicating that collected data will be kept confidential via limitations on the ability to share data by managerial means. The relatively close association of "Private Remedies," which generally indicates that the service provider will use internal methods to address confidentiality or privacy concerns, also indicates that such concerns are often viewed from the vantage point of agency responsibilities. The remaining clusters are far less compact, indicating a high level of distinctness for each cluster. This is, in part, reflective of the findings from the frequency analysis, which indicated that there is little consistency in the degree of information provided to consumers in the framework of this analysis.

4.4 Correspondence Analysis

For purposes of this analysis, correspondence will be looked at generally via the use of 2- and 3-D correspondence plots to allow graphical analysis based on the sub-categories identified in Table 1 above in the context of public, private, and ETC and electronic transit card policies. While individual keyword analysis can be performed, such analysis tends to create overly complex graphics, which are difficult to analyze. As this analysis is focused more generally on the presence of key concepts found within each type of policy, the decision has been made to focus on the overall clusters of interest found within each category. Additionally, case occurrences of sub-categories are analyzed in order to better identify how concepts correspond within policies. It is expected that there will be differences between the correspondence analyses of the policies analyzed, particularly in regard to enforcement and children's privacy, due, in part, to expectations reflected in policies relevant to public service providers. The following section will outline the findings of the correspondence analysis.

Graphical representations of correspondence allow for a more visual representation of the correspondences discussed above, and provide a clearer picture of how the privacy policies discussed here relate to one another and to the examined keyword categories. Two- and three-dimensional plots are created using cross-tabulations (or contingency tables) of rows and columns, where columns represent the category of policy studied, and rows represent the category of keyword (as seen in Table 1). The closeness of points in the chart represents similarity of row or column profiles. Lebart, *et al.* (1998) noted that, "According to usual notation, $f_{i.}$ designates the sum of the elements of row *i* and $f_{.j}$ is the sum of the elements of column j of this table. The profile of row *i* is the set of *p* values:

$$\left(\frac{f_{ij}}{f_i} \right), j = 1, \ldots, p$$

The profile of column *j* is the set of *n* values:

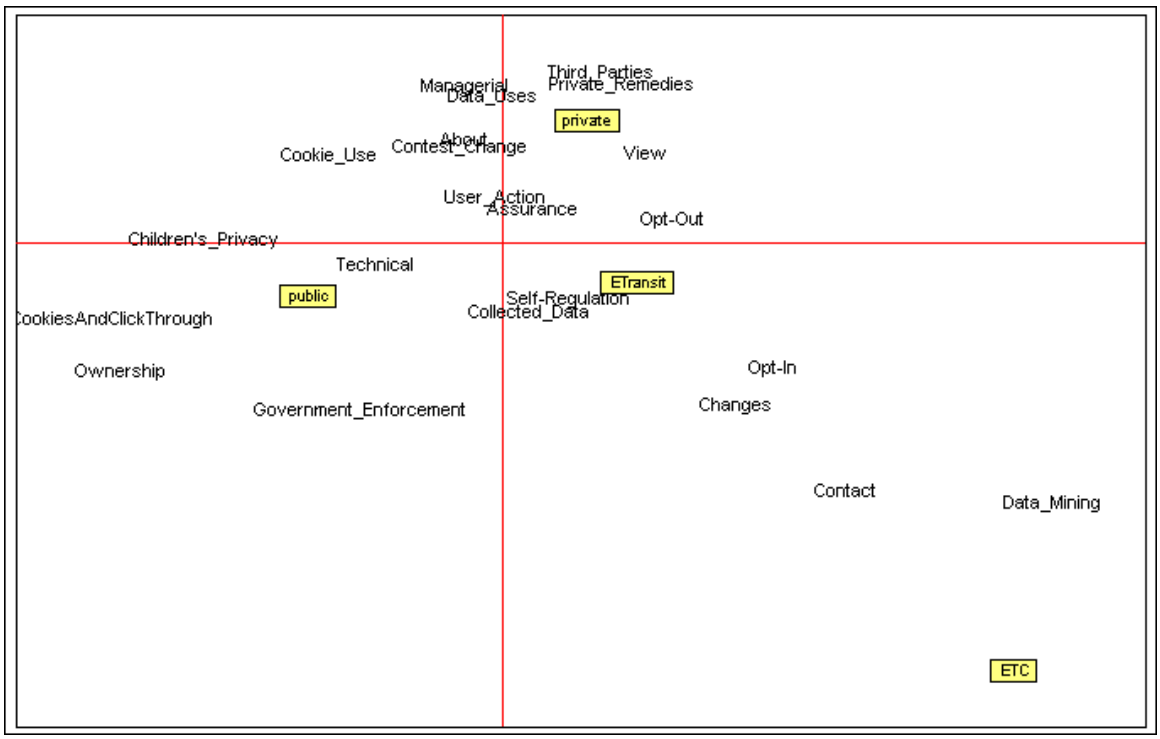
$$\left(\frac{f_{ij}}{f_{.j}} \right), i = 1, ..., n"$$

The origins of the axes in correspondence plots represent the marginals of the table of frequencies, with distance from the origin indicating singularity of items (in this case, privacy policy types). A visual representation of the contributing factors to this similarity or difference is found in the position of category keywords relative to the policies of interest. As with the policy categories, the location of a keyword category relative to the location of the origin or policy type indicates its' singularity relative to the overall distribution. Category and sub-category associations for public, private, ETC, and electronic transit card providers are presented in Figure 5. Disaggregated 2-D figures are shown in addition to the full 3-D plot, as the degree of correspondence between certain themes may make it difficult to fully ascertain their similarities.

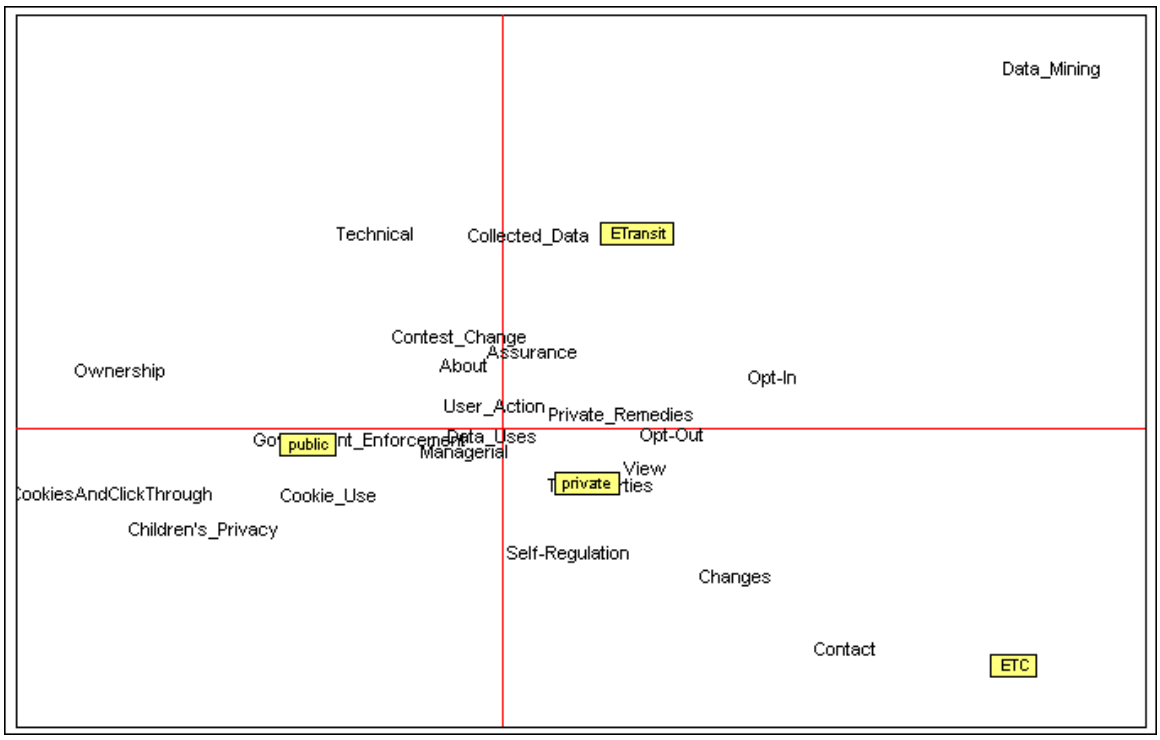
It is evident from these figures that significant differences exist in the types of policies examined here. In particular, ETC policies vary greatly with respect to the origin of the remaining three policy types along all axes, indicating that they display the most dissimilarity and the least inclusion of categories of interest. Given the discussion above, this is not a surprising finding; however, the degree of difference seen in the plot above indicates the degree of difference between each of the policy types in relation to the keyword categories studied. Here, distance from the origin indicates the relative singularity of items of interest. Table 3 below provides an overview of relative distance from the origin for both categories and variables of interest.

Figure 5: Correspondence Plot of Policy Concepts with Policy Types

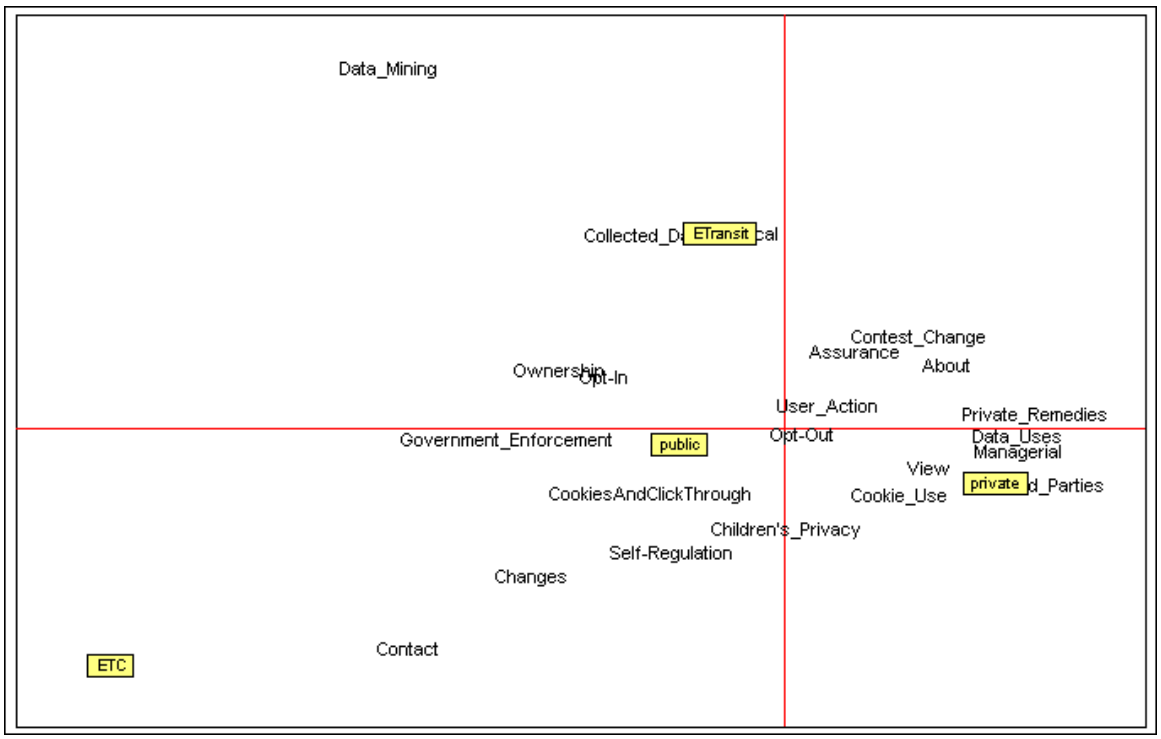
2-D Correspondence Plot: Axis 1 vs. Axis 2



2-D Correspondence Plot: Axis 1 vs. Axis 3



2-D Correspondence Plot: Axis 2 vs. Axis 3



3D Correspondence Plot

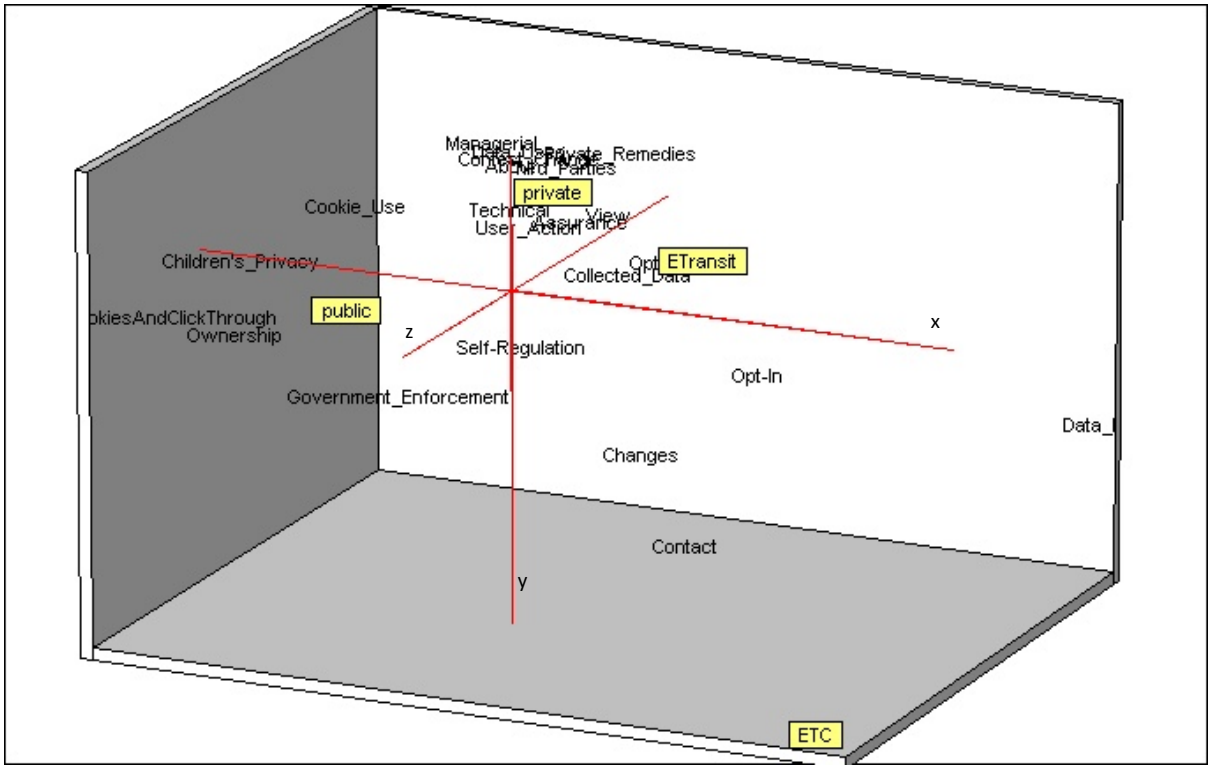


Table 3: Relative Distance (or Item Uniqueness) from the Axis of Origin of Privacy Policy Types and Content Categories

Variable Coordinates			
Item	**Axis1 (x)**	**Axis 2 (y)**	**Axis 3 (z)**
private	0.479	1.071	-0.546
public	-1.108	-0.528	-0.175
ETransit	0.763	-0.325	1.863
ETC	2.894	-3.409	-2.317
Category Coordinates			
Item	**Axis 1**	**Axis 2**	**Axis 3**
Contest_Change	-0.247	0.678	0.843
View	0.799	0.726	-0.431
Opt-In	1.533	-0.915	0.448
Opt-Out	0.954	0.087	-0.111
Contact	1.939	-1.906	-2.182
Government_Enforcement	-0.815	-1.411	-0.156
Private_Remedies	0.666	1.267	0.08
Self-Regulation	0.375	-0.574	-1.255
Managerial	-0.223	1.183	-0.28
Technical	-0.725	-0.233	1.836
About	-0.224	0.824	0.558
Assurance	0.158	0.348	0.683
Changes	1.317	-1.28	-1.49
Children's_Privacy	-1.692	0.008	-1.032
Collected_Data	0.145	-0.708	1.819
Cookie_Use	-0.992	0.578	-0.699
CookiesAndClickThrough	-2.225	-0.685	-0.682
Data_Mining	3.11	-2.006	3.436
Data_Uses	-0.058	1.183	-0.13
Ownership	-2.178	-1.145	0.508
Third_Parties	0.551	1.353	-0.6
User_Action	-0.053	0.216	0.169

Again, it is clear that the ETC category of privacy policies is the most singular of the policy types studied. In addition, contact, changes, opt-in and data mining are the most singular of categories. The charts and findings above indicate that while there is some consistency in topics addressed in overall privacy policies, there are some significant discrepancies in how well these topics are addressed by the various types of organization of interest. Such a finding, and the issues associated with these inconsistencies, indicates that there is scope for guiding policy that would bring more clarity and consistency to privacy policies. Particularly in the area of contact information and access to information, current practices leave the consumer with little information or ability to ensure that collected data are accurate and being used correctly.

The question of the singularity of ETC policies likely rests on a combination of factors. First, publicly available ETC privacy policies tend to be quite limited in scope. As noted above, these policies or language tend to consist of a short section within the context of a larger document, and tend to refer more broadly to overarching policies applicable to the state. One potential explanation for this is that because more traditionally “sensitive” data (in particular, financial data) are collected for ETC activities, ETC provision agencies are more cautious about promising protection of user data and thus prefer to keep language fairly vague. Another potential explanation is that ETC providers feel that the scope of their privacy protection is well addressed by other organizations (again, in particular financial) and that, as they must meet those privacy protections, there is no need to be additionally constrained. It is likely that each of these potential explanations plays some role in the

finding of the singularity of ETC privacy policies; however, additional examination of these agencies would be useful for greater understanding.

It is also evident from the plot and values shown that the overall structure of the "private" policies is most reflective of the general makeup of the policies as a whole. The clustering of keywords reflected by the value similarities of private policies along the axis supports the earlier finding that private policies tend to be most likely to contain reference to a broad segment of concepts identified through the FTC FIPPs. The public and ETransit categories, on the other hand, are closely related to specific concepts, but do not address as holistically the universe of privacy topics.

5. Findings

A number of findings may be drawn from the preceding analysis, particularly in relation to consistency and comprehensiveness. One key finding is that it is often difficult to obtain application or service-specific information on privacy policies related to data collected in the mobile environment. The lack of policies dealing specifically with location information gathered as part of application use or electronic transportation services (such as position information, trip routes traveled, or origin and destination information) indicates that there is currently little attention being given to location based privacy. While consumers are generally assured that any personal information they provide (such as name, address, or financial information) will be protected by the collecting agency, non-personal data (such as IP address or patterns of use) are often considered anonymous, and thus consumers are informed that they may be shared with other agencies, or released in aggregated forms. While this type of protection may be sufficient for static data, it becomes more problematic if location data such as origins, destinations, or travel paths are not specifically defined as personal or anonymous. If data collected via the use of ITS or LBS technologies are treated as anonymous data, they may be subject to lesser degrees of privacy protection, thus opening up the potential for misuse or loss of anonymity. The overall lack of policies specific to the treatment of these data is worrying, as it is likely that without specific guidelines directing appropriate uses, the minimal amount of protection will be afforded. Thus, a key finding of this study is that current policies are lacking in their treatment of location specific data.

The analysis here supports the earlier finding that there is very little consistency across privacy policies in how well they address privacy concerns as outlined by the Federal Trade Commission (FTC), and reveals that this is applicable to public as well as private organizations. In particular, policies were lacking in providing information related to how consumers may view or correct data that have been collected; what data may be shared with third parties; what procedures consumers should follow if they feel that their data have been mishandled; and issues associated with data ownership and data mining. Again, these findings indicate that there is an overall lack of comprehensiveness associated with locational privacy policies, particularly in regard to consumer expectations of protection. While consumer expectations are not addressed in detail here, it is reasonable to believe that consumers expect basic protections of personal data. While consumers may not demonstrate explicit awareness, privacy of personal data is a general expectation as shown by court findings related to the Fourth Amendment. If existing privacy policies do not demonstrate a comprehensive reflection of the expectations of the federal government and, in turn, consumers, it may be posited that a general framework for construction of privacy policies relevant to location

information should be developed, in order that consumers may develop accurate expectations regarding treatment of their data.

A third key finding is related to the differences in the content of the types of policies evaluated here; namely, private, public, ETC, and Electronic Transit Card. A lack of consistency across the different types of policies indicates that agencies and companies tend to value different types of information provided to consumers. For example, public agencies consistently address the issue of children's privacy in their policies, as mandated by federal regulation. Without this requirement, however, private agencies are far less likely to address this issue. The cluster analysis conducted revealed significant differences in how well issues of interest are addressed across policy types, with those policies related to the use of Electronic Toll Collection systems showing the lowest degree of attention paid to overall privacy issues. Discrepancies across the range of policies analyzed indicate that consumers have very little consistent protection or information on which to base their expectations of privacy in the mobile network, thus it may be inferred that service agencies are not successfully meeting their responsibilities in regard to ensuring adequate protection of privacy.

6. Conclusions

As shown above, there are large discrepancies in how agencies, organizations and companies involved with the collection of travel data treat those data. Significant findings from the content analysis of privacy policies include recognition that considerable differences exist in how privacy is treated in public and private contexts, which may lead to difficulties in leveraging the use of one for benefits for both. If public agencies, for example, are to access and use data collected by private agencies, or vice-versa, significant problems may be encountered related to the potential for mining consumer information and revealing potentially sensitive information. With a lack of consistent guidance related to all aspects of data privacy in the mobile environment, including notification/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress, it is difficult for providers of ITS and LBS services to effectively plan and prepare for effective data protection.

The lack of consistency evident in the policy analysis carries with it implications for future implementation of ITS and LBS systems, as well as ubiquitous networked mobility systems. If policy-makers and the general public are not confident that collected data will be treated in a manner in keeping with privacy expectations of the general public, it is likely that funding and implementation of such systems will be stymied until such time as adequate protections are in place. By acknowledging the failures of the current approach, it may be possible to identify needed protections and begin the process of developing both technological protections that may be built into future systems, as well as developing policy guidance to ensure that these protections are adhered to. Addressing needs associated with differing operational models in the public and private environments will also be necessary if public-private partnerships are to be developed. Such inconsistencies are also detrimental to the ability of consumers to determine accurate expectations of privacy in the mobile environment, or effective ways of mitigating privacy risks.

The emergence of low-cost GPS technologies and mobile applications on smartphones has brought the public environment into the private sphere, which creates uncertainty in relation to chains of data creation, awareness, ownership and sharing, topics not effectively or clearly covered by the policies studied here. The lack of information regarding ownership, in particular, is a difficult matter to address, as most privacy policies evaluated either do not refer to who owns the data, or explicitly state that collected data are owned by the collecting entity. While most policies do indicate that collected data may be shared by the collecting entity for purposes of law enforcement, the degree of information collected may not be adequately presented to the consumer. In such cases, the expectations of the service user may be at odds with the practices of the collecting entity. Here, additional clarity with respect to collected data and potential uses would be of use to the consumer and the courts, as it would allow for more reasonable expectations to be developed. These expectations could be managed in the following ways:

1. Inform consumers of specific types of data that may be collected: While many privacy policies inform consumers that their name, email address, and various travel data may be collected, many others make only vague references to types of data that may be obtained via use of the service or application. Provision of more specific data regarding what data (in particular, location data) may be collected may provide consumers with the ability to develop more informed expectations regarding types of data that may be collected.
2. Inform consumers of potential for data uses: As shown above, consumers are currently not provided adequate information regarding how their data may be used by collecting agencies. Additional information regarding the potential for use by third parties, in legal contexts, and for transportation benefits (such as safety increases and efficiency improvement) may give consumers scope for making more informed decisions regarding the sharing of data. Publishing agreements between collecting entities and those with whom they share data would also be useful in this context, as this would provide consumers with better information with which to make decisions relevant to sharing of data and expectation of privacy risks.
3. Provide consumers with clear information regarding data ownership: Indicate to consumers what data will be generated via use of the service or application, and indicate specifically the agency that will be considered to be the “owner” of said data. Provide specific information regarding the extent of this ownership, including allowed uses and management in the case of account termination.
4. Provide companies with clear direction regarding federal expectations towards data collection and use: Here, it may be helpful to develop an overarching policy that explicitly addresses expectations of collection, storage, management and use of data obtained through consumer use of mobile applications and services.

The methods proposed here would, it is hoped, address some of the issues identified in the preceding analysis, and provide clearer guidance to those entities involved with the collection of data in the mobile environment. While point 4 above refers more specifically to the US federal expectations, it should be noted that each of the above recommendations may be implemented under any geographic scope. It should be noted that doing so would provide immense benefits to both consumers and agencies worldwide, by implementing more standard practices into the realm of location data.

References

1. Ardagna, C.A., M. Cremonini, S. De Capitani di Vimercati, and P. Samarati (2011). "An Obfuscation-based Approach for Protecting Location Privacy," in IEEE Transactions on Dependable and Secure Computing (TDSC).
2. "Ban, X. and M. Gruteser (2010). ""Mobile Sensors as Traffic Probes: Addressing Transportation Modeling and
3. Privacy Protection in an Integrated Framework. 7th International Conference on Traffic & Transportation Studies."
4. Berelson, B. (1974). Content Analysis in Communication Research. New York: Free Press.
5. Cottrill, C. D. (2011). Location Privacy: Who Protects?. URISA Journal-Urban and Regional InformationSystems Association, 23(2), 49.
6. Cottrill, C.D. and P. Thakuriah (2011). Protecting Location Privacy. Policy Evaluation. In Transportation Research Record, Journal of the Transportation Research Board, No. 2215, pp. 67-74.
7. Directions Magazine (2010). Location Based Services. Available at http://www.directionsmag.com/companies/category/Location_based_Services_%28LBS%29/.
8. ESRI (2002). Cluster analysis tool. Accessed at: http://edndoc.esri.com/arcobjects/8.3/Samples/Analysis%20and%20Visualization/Cluster%20Analysis/CLUSTERANALYSIS.htm.
9. Graneheim, U.H. and B. Lundman (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. Nurse Education Today, 24, Pp. 105–112.
10. Halliday, J. (2011). Google agrees to privacy reviews to settle Buzz complaint. guardian.co.uk, Wednesday 30 March.
11. Hansen, M. (2008). "Privacy and Identity Management." IEEE Security and Privacy. 1540-7993. 38-45.
12. Harris Poll for TRUSTe (2011). Smart Privacy for Smartphones: Understanding and delivering the protection consumers want.
13. Helft, M. (2010). Facebook Acknowledges Privacy Issue With Applications. The New York Times. October 18.
14. Hui, K.L. and I.P.L. Png (2006). The Economics of Privacy. Economics and Information Systems, Handbooks in Information Systems, Vol. 1, Chapter 9, ed. Terrence Hendershott. Elsevier.
15. Karvonen, H. (2010). Different Aspects of Trust in Ubiquitous Intelligent Transportation Systems. Proceedings of ECCE 2010 Conference, Delft, The Netherlands. Pp. 311-314.
16. Kassarjian, H.H. (1977). Content Analysis in Consumer Research. The Journal of Consumer Research. Vol. 4, No. 1, pp. 8-18.
17. Khalifa, A. A.; M. Haranczyk and J. Holliday (2009). Comparison of Nonbinary Similarity Coefficients for Similarity Searching, Clustering and Compound Selection. J. Chem. Inf. Model. 49, 1193–1201.
18. Lebart, L., A. Salem and L. Berry (1998). Exploring Textual Data. Dordrecht, The Netherlands: Kluwer Academic Publishers.

19. Liu, C., J.T. Marchewka, J. Lu and C.-S. Yu (2004). Beyond concern: A privacy–trust-behavioral intention model of electronic commerce. Information & Management, 42, 127-142.
20. Liu, L. (2009). Privacy and location anonymization in location-based services. SIGSPATIAL Special, 1(2): 15-22.
21. McKay, C. (2012). "Letter to Google refarding privacy policy changes." Office of the Privacy Commissioner of Canada. Accessed at: http://www.priv.gc.ca/media/nr-c/2012/an_120224_e.cfm.
22. Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. Journal of Computer-Mediated Communication, 9(4), article 1.
23. National Association of Attorneys General (2012). Letter to Larry Page, Google CEO. Accessed at: http://www.naag.org/assets/files/pdf/signons/20120222.Google%20Privacy%20Policy%20Final.pdf.
24. Nuendorf, K.A. (2002): The Content Analysis Guidebook. Thousand Oaks, California: Sage Publications.
25. Potoglou, D, Robinson, N, Kim, C-W, Burge, P & Warnes, R (2010). Quantifying individuals' trade-offs between privacy, liberty and security: the case of rail travel in UK. Transportation Research. Part A: Policy & Practice, 44, 169-181.
26. Provalis Research (2010). WordStat - Content analysis module for SIMSTAT and QDA miner. Montreal, QC.
27. Shapiro, S.S. (2012). Situating Anonymization Within a Privacy Risk Model." IEEE.
28. Shilton, K. (2009). Four Billion Little Brothers? Privacy, mobile phones, and ubiquitous data collection. UC Los Angeles: Center for Embedded Network Sensing. Retrieved from: http://escholarship.org/uc/item/2xr2r802
29. Sneath, P.H.A. and R.R. Sokal (1973). Numerical Taxonomy. W.H. Freeman, San Francisco.
30. Sydney Morning Herald (2012). "Heat turned up on Google's privacy blur." Accessed at: http://www.smh.com.au/technology/security/heat-turned-up-on-googles-privacy-blur-20120306-1uf4v.html.
31. Thurm, S. and Y.I. Kane (2010). "Your Apps are Watching You." The Wall Street Journal. Accessed at: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html
32. U.S. Department of Education (2002). Adult Literacy in America (NALS). National Center for Education Statistics, U.S. Dept of Education, Office of Educational Research and Improvement (NCES 1993-275).
33. U.S. Federal Trade Commission (2007). Fair Information Practice Principles. http://www.ftc.gov/reports/privacy3/fairinfo.shtm.
34. Xu, H., Teo, H. H., Tan, B.C.Y., and Agarwal, R. (2010). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services, Journal of Management Information Systems, Vol. 26, No. 3, pp. 135–173.
35. Zyskowski, J. (2011). Apple iPhone becomes lightning rod for public's privacy fears. Federal Computer Week. May 5th.