Desperately Seeking Assurances: Segmenting Users by their Information-Seeking Preferences

A Q Methodology Study of Users' Ranking of Privacy, Security & Trust Cues

Anthony Morton
Department of Computer Science
University College London
London, United Kingdom
anthony.morton.09@ucl.ac.uk

M. Angela Sasse
Department of Computer Science
University College London
London, United Kingdom
a.sasse@cs.ucl.ac.uk

***Abstract*—Users of technology services try to evaluate the risks of disclosing personal information in light of the benefits they believe they will receive. However, because of cognitive, time or other constraints, users concentrate on minimizing the uncertainties of disclosure – reducing their level of privacy concern – by using a limited set of information cues. We suggest an individual's information-seeking behavior is focused on those cues which are important to them. Q methodology was used to determine if users of technology services can be segmented, based on the type of information cues they consider important – many of which are related to technology services' privacy behavior. The study consisted of 58 participants split into two cohorts, who rank-ordered 40 statements describing the attributes of a technology service. In our study, 69% of participants loaded significantly into only one of five groups: 1) *Information Controllers*; 2) *Security Concerned*; 3) *Benefits Seekers*; 4) *Crowd Followers*; and 5) *Organizational Assurance Seekers*. Only 12% of participants did not load significantly into any of the five groups. Our findings assist practitioners in understanding how their privacy behavior (e.g. repurposing information) and privacy-sensitive technology design (e.g. providing feedback and control mechanisms) could encourage or discourage the adoption of technology services by different types of users. We argue the user segmentation identified by this study can inform the construction of more holistic privacy personas.**

Keywords—information privacy, Q methodology, information-seeking behaviors, privacy concern, trust

I. INTRODUCTION

An oft-quoted piece of advice to presenters is that they "*must know their audience*". *Technology services*[1], such as an e-commerce website, social networking or smartphone application, often request personal information in return for benefits (e.g. access to required information, social contact, entertainment, discounts, etc.). Existing non-contextual measures of privacy concern do not assist organizations providing technology services to understand what is important to their audience – particularly in terms of the organization and technology's privacy behavior. Users of technology services have expectations and assumptions when first engaging with a technology service. If its privacy behavior does not match those expectations (e.g. the user is unaware that data about them is being collected and shared with other parties), they may respond emotionally and reject it, or distrust the motives of the providing organization [2], [3]. Organizations need to understand how their privacy behavior – particularly their *ability* and *motivation* [4] to safeguard peoples' personal information – encourages or discourages acceptance of their technology services, and users' willingness to provide personal information. Furthermore, organizations need to appreciate the differing importance users attach to various aspects of a technology service – particularly those relating to its privacy behavior; they must therefore truly '*know their audience*'.

Existing privacy concern measures, like Concern For Information Privacy (CFIP) [5] and Internet Users Information Privacy Concern (IUIPC) [6] – two of the more influential [7] – offer the practitioner limited assistance in understanding the cues people seek to assess whether an organization can be trusted with their personal information [4], [8]. Privacy concern measures usually exclude users' expectations, assumptions and perceptions of the providing organization [2], which are often influenced by information cues, such as its prominence, reputation or brand image [9]. For example, an individual's concern about the *collection* of personal information – a sub-scale in CFIP and IUIPC – is likely to be influenced by their perception of an organization's ability and motivation. Existing privacy concern measures also ignore the nature of the technology platform used in a technology-mediated transaction [10].

This paper describes an innovative use of Q methodology in privacy and trust research, where participants ranked statements describing aspects of an 'ideal' generic technology service – particularly its privacy behavior – in order of importance to them in their decision to use it, and provide it with their personal information. Q methodology is a research method combining qualitative and quantitative approaches – first developed by Stephenson [11] – and used in social sciences and psychology to investigate peoples' subjective viewpoints. Given the subjective nature of privacy [2], we believe it is an appropriate research method for investigating what most and least influences peoples' decision to use a

[1] A technology service is a socio-technical system consisting of a technology platform – referred to as the *technology lens* – and its providing organization [1].

Anthony Morton is funded by a PhD scholarship – part of a UK Engineering and Physical Sciences Research Council (EPSRC) grant (EP/G034303/1) – awarded to the Centre for Secure Information Technologies (CSIT) at Queen's University, Belfast.

technology service, and determining if salient groupings can be identified. For example, unless solely focused on the benefits provided by a technology service, some people will seek organizational assurances – possibly in the form of its privacy policy [8] – whilst others will ask friends and family.

The majority of statements used in the study are structured around a framework for organizational privacy practice previously proposed by the authors [1]. The results from this study therefore assist practitioners in understanding which aspects of their privacy practice are most and least likely to influence users' decision making.

II. Related Work

An individual's use of a *technology service* can be viewed as a technology-mediated interaction between an *information sender* (e.g. an individual) and an *information receiver* (e.g. an organization) via a technology platform (e.g. an e-commerce website). Technology-mediated interactions usually take place because the information sender has goals, and must balance the risks of relinquishing some aspect of their information privacy against their need to achieve these goals (e.g. releasing their location to a restaurant-finder smartphone application). Olivero & Lunt concluded from their study of information disclosure in e-commerce exchanges that "[…] *an emerging theme is that of a diffused lack of trust in e-commerce exchanges leading to a pragmatic evaluation of costs and rewards associated with disclosure*" [9, p. 258]. This echoes Culnan & Bies who observed that individuals "*disclose personal information as long as they perceive that they receive benefits that exceed the current or future risks of disclosure*" [12, p. 327]. With reference to Berger & Calabrese's Uncertainty Reduction Theory, Beldad *et al* [8] suggest an individual's uncertainty about the risks of information disclosure triggers privacy concerns, leading to *information-seeking behaviors*. They observe, "*uncertainties cause discomfort, people seek to eliminate them by acquiring pertinent information*" – with privacy policies often being the only resource [8, p. 222].

Even if perfect information about a technology service is feasible, bounded rationality and psychological factors will influence an individual's decision making [13], and they will concentrate on finding information about the attribute(s) of a technology service they consider important. If they are unable to do so, or can only find limited evidence, their level of privacy concern is likely to increase. For example, individuals who *do* read privacy policies may become concerned if the providing organization does not have one, or its description of information use is ambiguous. Similarly, individuals may seek environmental cues relating to a technology service, with their level of concern increasing if none of their friends have used it [10]. These concerns are underpinned by an individual's *dispositional privacy concern* [14]. Users "*who have totally submitted to the belief that information disclosure is extremely risky*" are unlikely to be influenced to share information [8, p. 228] – even if a technology service's privacy policy embodies fair information practices.

One of the authors has previously proposed a *grammar of privacy concern* (Fig. 1) [10], which uses a similar approach to McKnight & Chervany's *grammar of trust* [15], with three layers: 1) dispositional privacy concern – "*an individual's innate concern about disclosing any information to other parties*"; 2) environmental privacy concern – "*an individual's level of privacy concern created from environmental cues, such as media reports, anecdotes from friends and family, and social privacy norms*"; and 3) interpersonal privacy concern – "*an individual's level of privacy concern about the party they are transacting with*" [10, pp. 267–268]. The shading in Fig. 1 represents the increasing influence of context on each layer. Context has most influence on an individual's privacy concern about a specific information sender, but a weak influence on their dispositional privacy concern.

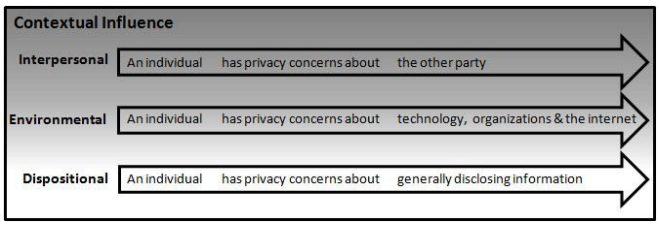

Fig. 1. Grammar of Privacy Concern. Based on [10]

In a technology-mediated interaction, an information sender (*trustor*) must decide whether to trust the information receiver (*trustee*) with their personal information, in return for the benefits of using a technology service. Mayer *et al* define trust as, "*the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"* [16, p. 712]. When initially engaging with a trustee, a trustor will form a perception of the trustworthiness of the trustee based on the *trust signals* emitted by the trustee [4]. These trust signals include *trust symbols* (e.g. use of the HTTPS padlock and trusted third party seals), and *trust symptoms* (e.g. user reviews and the design of the technology service) [4]. Trust signals are typically only used during the first few transactions between trustor and trustee. After this the trustor expects the trustee to fulfill their obligations, and will not consider there to be a risk.

We suggest a trustor uses trust signals to ascertain a trustee's likely privacy behavior. If the trustee's privacy behavior deviates from the trustor's expectations (e.g. collected information is repurposed), they may respond emotionally, distrusting the trustee's motives [2], [3]. At the interpersonal layer (Fig. 1) a trustor is therefore likely to seek evidence of the trustee's *ability* and *motivation* [4] to safeguard their personal information. At the environmental cues layer (Fig. 1) a trustor may seek comfort from a technology service being used by friends or family, or positive media reports about similar technology services.

We previously proposed a framework for effective privacy practice, which unifies an organization's ability and motivation in safeguarding personal information [1]. For a technology-mediated interaction between an information sender and information receiver, our layered Privacy Security Trust (PST) Framework unifies in one model: 1) the delivery of effective privacy practice within the information receiver; 2) the construction of trust between the information sender and

information receiver; and 3) the characteristics of the technology platform used. The PST Framework represents effective privacy practice as five layers: 1) *information security* – protecting information assets from threats; 2) *information management* – providing control over information assets; 3) *information principles* – describing the rules which guide an information receiver in using its information assets; 4) *information use* – defining the use to which an information receiver will put the information assets in its possession; and 5) *information privacy culture* – assisting the information receiver in making decisions about which information assets to collect, store, process, disseminate and share.

III. Research Questions & Method

A. Research Questions

The study's primary research objective was to investigate if salient groupings could be identified based on the relative importance people attach to information about: 1) a technology service's privacy behavior; 2) a technology service's facilities for feedback and control of personal information; 3) any consequences of using a technology service; 4) the benefits of using a technology service; 5) protection if problems occur using a technology service; 6) the attributes of a technology service; and 7) environmental cues (e.g. the advice of friends and family).

Two of the principal criticisms of Q methodological studies is their reliability and generalizability [17]. However, concerns about replicability – an important form of reliability – where similar viewpoints emerge across different Q samples, have been found to be unwarranted [17]. Nevertheless, a secondary research objective was to ascertain if similar salient groupings could be identified from two samples of participants using different implementations of the same experiment.

B. Use of Q Methodology

Q methodology uses stimuli – implemented as a set of statements called a 'Q-set'[2] – representative of a wide breadth of discourse about a research topic or issue of interest. Participants – the 'P-sample' – are asked to rank the statements in a Q-set – a process called 'Q-sorting' – in an order which is important or relevant to them[3] using a forced distribution grid – typically quasi-normal (Fig. 2). This has the advantage that statements people find *most* important are equally psychologically significant to those they find *least* important [18]. It also prevents participants from selecting all statements as important – a common problem with surveys. Q methodology uses by-person factor analysis of the intercorrelated matrix of Q-sorts – the ranking of statements by each participant – to group them into factors that are statistically similar, i.e. participants in a factor are those who ordered statements similarly.

The specific rankings of individual statements using Q methodology have been shown to be broadly similar to those produced by a Likert attitude scale [19]. However, Q methodology not only "*distinguish*[es] *salient groupings within the population with similarly structured attitudes towards an image object*", but "*results in segmentation on the basis of functional content-specific criteria*" [19, p. 516] – essential for the study's primary research objective.

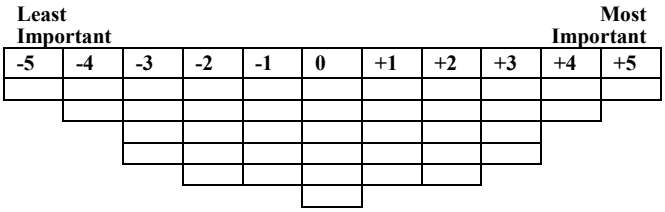

Fig. 2. Forced distribution for Q-sorting used in the study

A characteristic of Q methodology is that sample sizes are small (i.e. 10-20 participants). A typical ratio of statements to participants is 1:3 (i.e. three participants in the P-sample for each Q-set statement), but this can drop to 1:2 [20]. Another useful heuristic is that at least three participants should load significantly on a factor [20]. As Brown [21] observes, "*since the interest of Q methodology is in the nature of the segments and the extent to which they are similar or dissimilar, the issue of large numbers, so fundamental to most social research, is rendered relatively unimportant.*". A Q methodological study only requires sufficient participants to establish the existence of a factor, and be able to delineate it. The problem – inherent in normal factor analysis – of whether a sample is sufficiently large to be generalisable to a wider population does not afflict Q methodology [22].

C. Construction of Concourse and Q-Set

The first step in Q methodology – the creation of a *concourse*, of which the Q-set is a subset – used transcripts from an earlier qualitative study by one of the authors in which privacy-affecting technology services were discussed by focus groups [10]. The focus groups' transcripts were coded using ATLAS.ti, with 73 base-level codes grouped into 16 super-codes. To investigate the primary research question, ten of the 16 super-codes relate to quotations in the focus group transcripts relating to the organization and technology lens components of the PST Framework [1]. The remaining six codes relate to quotations about: 1) consequences for the individual of using a technology service; 2) an individual's privacy calculus; 3) legal protection for the individual; 4) features of a technology service; 5) environmental cues; and 6) benefits provided by a technology service.

A structured Q-set was created using a *balanced-block* approach [22, p. 59], with 40 statements split into 15 sub-categories representing 15 of the 16 ATLAS.ti super-codes[4]. The statements within each category represent the base-level codes with the largest number of coded quotations. Use of the balanced-block approach ensured that just over half of the statements relate to a technology service, with 13 statements mapped to the six sub-categories in the *organization* component of the PST Framework [1], and 10 mapped to the four sub-categories in the *technology lens* component. The remaining 17 statements are split approximately equally across the remaining five categories (Table IV).

[2] Sometimes called a 'Q-sample'.

[3] In the study, participants ranked Q-set statements from 'Most Important' (+5) to 'Least Important' (-5) using the grid shown in Fig. 2.

[4] Privacy calculus is a cognitive process, and not something an individual might seek for reassurance; it was therefore excluded from the concourse.

The Q-set statements are positively worded to avoid the problem of participants trying to rank negatively-worded statements. It also forces them to consider the factors which are particularly important and unimportant to them, when faced with an 'ideal' technology service. In addition, the statements and participant instructions make no reference to specific technology services, to minimize the potential effect of organizational reputation.

D. Sampling

One of the research objectives was to investigate if two different implementations of the Q-sort produced broadly similar results. The study's P-sample was therefore split into two approximately equal-sized cohorts: 1) an online cohort – who used an online Q methodology tool called FlashQ[5] to perform their Q-sort; and 2) an offline cohort – who carried out their Q-sorts using a printed Q-set under laboratory conditions at University College London (UCL). The demographic profile of the two cohorts is shown in Table I.

TABLE I. PARTICIPANT PROFILE OF ONLINE & OFFLINE COHORTS

Demographic Characteristic	Category	Online Cohort ($N = 27$)	Offline Cohort ($N = 31$)
Gender	Male	48%	32%
	Female	52%	68%
Age (years)	18-24	37%	61%
	25-34	11%	10%
	35-44	19%	13%
	45-54	19%	10%
	55-64	15%	3%
	Over 65	0%	3%
Maximum level of education achieved	School leaver	15%	11%
	Diploma	19%	37%
	Undergraduate	37%	37%
	Postgraduate	22%	15%
	Rather not say	7%	0%
Computer Experience (years)	Mean	19.1	14.5
	Standard Deviation	8.7	5.2

1) Online Cohort

The online cohort, which took place between March and July 2013, was sampled from two sources:

1. Structured sampling of participants who completed an online survey ($N = 140$) investigating attitudes about personal information and technology adoption[6].
2. Structured sampling of an opportunistic sample of participants ($N = 26$) who completed an online survey including the *Desire for Privacy (DFP)* and *Concern about Privacy Behavior of Organizations and Governments* (CPBOG) measurement instruments, previously piloted by one of the authors [14][6].

To minimize the homogeneity of the online cohort, 50 participants were selected randomly within different levels of privacy concern measured by these two online surveys. Of the 50 participants, 39 completed the study. To mitigate the possibility that some of the 39 participants may not have read the Q-set statements carefully, or given them proper consideration, 12 of the 39 Q-sorts – completed in less than 70% of the cohort's mean completion time[7] – were excluded.

2) Offline Cohort

The offline cohort, which took place between September and October 2013, consisted of 31 participants – mostly from UCL's Psychology Subject Pool – who volunteered for the study; no structured sampling of this cohort took place.

E. Research Method

Participants in the offline cohort completed a paper-based survey at the start of their session requesting demographic information and asking them to complete the DFP and CPBOG measurement instruments [14]. The remainder of the process for the offline and online cohorts was the same, thus:

1. If participants had started using a technology service in the last six months, they were asked to provide the name of the technology service, and up to three reasons why they felt comfortable to use it and provide it with their personal information[8].
2. Participants were told to think generally about technology services, given the 40 Q-set statements in random order, and asked to sort them into three piles: 1) most important; 2) least important; and 3) neutral, in their decision to use a technology service.
3. Participants were asked to place the Q-set statements from the three piles on the Q-sort grid (Fig. 2).
4. Once the participant had completed their Q-sort, they were asked to provide the reasons why they had ranked a particular statement as +5, and another as -5.

The Q-sorts took approximately 30-35 minutes, for which participants were paid the equivalent of US$8. The study was approved by the designated ethics officer in the Computer Science Department at UCL, who decided it did not require full ethical clearance from UCL's Ethics Committee.

IV. FACTOR ANALYSIS

A. Onlineand Offline Cohorts - Initial Analysis

It was hypothesized that there should be no significant difference in the distributions of the online and offline cohorts, when taken as a whole (i.e. the two cohorts should rank the statements in broadly the same order). A Mann-Whitney U test showed there was no statistically significant difference in the scores for each of the 40 statements for the online and offline cohorts, with results ranging from U = 414; $z = -0.071$; $p = 0.94$ ($sig \leq 0.05$, 2-tailed) for statement 30 to U = 305; $z = -1.79$; $p = 0.074$ ($sig \leq 0.05$, 2-tailed) for statement 38.

A Principal Components Analysis (PCA) was run separately on the two cohorts' Q-sorts using PQMethod[9] to

[5] FlashQ – originally developed by G. Braehler and C. Hackert – allows participants to carry out Q-sorts using a web browser (see http://www.hackert.biz/flashq/home/). A newer version – updated by R. Hoodenpyle – was used in the study (see http://qmethod.org/links).

[6] Participants completing these two online surveys were informed that they might be selected to complete a future online exercise.

[7] This was approximately 11 or 13 minutes, depending on whether a participant had entered reasons for starting to use a technology service.

[8] The analysis of this data is outside the scope of this paper.

[9] Peter Schmolck, PQMethod Version 2.33 (December 2012) available at http://schmolck.userweb.mwn.de/qmethod/downpqwin.htm.

ascertain the number of factors to initially extract using centroid analysis. Statistical tests, including Kaiser-Guttman's criterion, the existence of at least two significantly loading (≥ 0.41) Q-sorts, Humphrey's rule[10] and Cattell's scree test [22] indicated that between four and six factors should be extracted from the offline cohort, and seven from the online cohort.

B. Offline Cohort – Centroid Factor Analysis

Six factors were initially extracted using centroid factor analysis – the preferred method of Q practitioners [22] – from the 31 Q-sorts in the offline cohort. There was no theoretical foundation for manually rotating the factors subjectively, so varimax rotation was used to achieve the best mathematical fit. This resulted in the first four, and the sixth factors having five or more significantly loading Q-sorts; the fifth factor was therefore discarded as it had none. The five-factor solution explains 46% of the study variance – a "*sound solution on the basis of common factors*" [22, p. 105] – with 21 Q-sorts (68%) loading significantly on only one factor; the factors' inter-correlations are shown in Table II. Although Factor 4 is a bipolar factor – with one significantly loading Q-sort at its negative pole and four at its positive pole – this is not considered a problem [22]. There are seven confounded Q-sorts and three Q-sorts not loading significantly on any factor.

TABLE II. INTER-CORRELATIONS BETWEEN OFFLINE FACTOR SCORES

Factor	1	2	3	4	5
1		0.554	0.295	-0.042	0.680
2	0.554		0.223	0.144	0.455
3	0.295	0.223		0.387	0.225
4	-0.042	0.144	0.387		0.057
5	0.680	0.455	0.225	0.057	

C. Online Cohort – Centroid Factor Analysis

Seven factors were initially extracted using centroid factor analysis from the 27 Q-sorts in the online cohort. Varimax rotation resulted in six factors, each with two or more significantly loading Q-sorts. One factor had no significantly loading Q-sorts and another only two. A second centroid factor analysis was therefore run extracting six factors. This resulted in the first three, the fifth and sixth factors having at least three significant loadings; the fourth factor was therefore discarded.

TABLE III. INTER-CORRELATIONS BETWEEN ONLINE FACTOR SCORES

Factor	1	2	3	4	5
1		0.395	0.552	0.363	0.161
2	0.395		0.481	0.389	0.350
3	0.552	0.481		0.340	0.210
4	0.363	0.389	0.341		0.230
5	0.161	0.350	0.210	0.230	

The five-factor solution explains 48% of study variance, with 20 Q-sorts (74%) loading significantly on only one factor; the factors' inter-correlations are shown in Table III. There are four confounded Q-sorts, and three Q-sorts not loading significantly on any factor.

[10] Humphrey's rule was strictly applied, where the cross-product of the absolute value of the two highest loadings in a factor should be greater than twice the standard error.

D. Factor Interpretation & Alignment

Watts & Stenner [22] suggest the use of a data-driven crib sheet for highlighting items of importance in the factor array produced by Q-sort analysis, in line with Stephenson's belief that Q methodology should be a holistic procedure, rather than a reductionist, statement-by-statement approach. To aid factor interpretation, a *crib worksheet* was developed in Microsoft Excel® for each factor in a cohort to highlight: a) statements ranked +5 or -5; b) statements ranked higher or equal highest; and c) statements ranked lower or equal lowest, by that factor. The crib worksheet was then used to create the factor narratives through a process of abduction.

Unlike typical Q methodology studies which use a single sample, our study had two cohorts. One of the research objectives was to determine if the online and offline Q-sorts produced broadly similar groupings of participants (i.e. factors). This made analysis particularly challenging, as two factors (one from each cohort) would be unlikely to rank statements exactly the same. Nevertheless, if a factor from one cohort ranked statements in a category between +4 and +5, a potentially equivalent factor from the other cohort should rank most (if not all) of the statements in the same category positively and within one position, i.e. between +3 and +4. A Microsoft Excel® *factor comparison spreadsheet* was developed to highlight where factors from the offline and online cohorts both ranked the same statement: a) highest in their cohort; b) lowest in their cohort; c) neutral or ±1; d) higher than +1 and within one position; or e) lower than -1 and within one position. Determining which factors from the two cohorts most closely aligned was performed, thus:

1. The *crib worksheet* of an unaligned factor in the offline cohort (Factor X) was used to determine the category with the most statements ranked highest and very few (or no) statements ranked lowest – this was the principal focus of Factor X.
2. The *factor comparison spreadsheet* was used to find a factor from the online cohort (Factor Y) with the most statements in the same principal focus category ranked higher than the other factors in its cohort. The statements which the offline and online factors ranked lowest were also checked to confirm broad agreement.
3. The degree of agreement between Factor X and Factor Y concerning statement ranking was checked using the *factor comparison spreadsheet*. Factors were considered to be aligned when the number of statements they ranked similarly was higher than possible alignments with other factors. Occasionally, it was necessary to subjectively relax this criterion to satisfy step 2.

The alignment and composition of the five factors is shown in Tables IV and V. Full factor narratives are provided in Section VII for the two factors with the largest number of significantly loading Q-sorts, with the appropriate Q-set statement references (Table IV) provided in parentheses for each part of the narratives; the remaining three factors are provided as summary interpretations. To illustrate the essence of each factor, the narratives also include participants' reasons for ranking particular statements as +5 or -5.

TABLE IV. CATEGORIZED Q-SET STATEMENTS, OFFLINE AND ONLINE COHORT FACTOR ARRAYS, AND FACTOR ALIGNMENT[a]

CATEGORY	Sub-Category	Ref.	Q-Set Statement	Information Controllers		Security Concerned		Benefit Seekers		Crowd Followers		Org. Assurance Seekers	
				Offline Factor 1	Online Factor 4	Offline Factor 2	Online Factor 1	Offline Factor 3	Online Factor 5	Offline Factor 4	Online Factor 2	Offline Factor 5	Online Factor 3
Organization	General	1	The organization has a good reputation	**0**	**-3**	**+3**	+2	+2	+1	**+3**	**+4**	**0**	0
	General	2	The organization is of a suitable size for the technology service it is offering	-4	-2	-3	**0**	**-5**	-4	**-1**	-5	-2	-2
	General	3	The organization appears to be competent	**-3**	-1	-1	**-2**	-2	**+2**	**+2**	0	-2	-1
	Information Privacy Culture	4	The organization tells me it will not mislead me about the collection and use of my personal information	+1	**-2**	**+3**	0	**-3**	-1	-2	-1	+2	**+4**
	Information Privacy Culture	5	The organization tells me it takes looking after my personal information seriously	0	**-4**	0	+1	**-3**	+1	**-3**	-2	**+1**	**+3**
	Information Use	6	The organization will tell me which items of my personal information it is going to share with other organizations, and why	+2	**+3**	+2	**0**	**0**	+1	**0**	**+3**	**+3**	+1
	Information Use	7	The organization will ask me before it uses my personal information for any purpose other than what it was originally collected for	+3	**+4**	+3	+3	**0**	**-3**	+1	+1	**+4**	+1
	Information Principles	8	The organization's terms and conditions for using the technology service are easy to understand	**-2**	-4	**-2**	**-2**	-4	**-5**	**-5**	-4	-3	**-2**
	Information Principles	9	The organization seems to follow applicable laws and regulations	**-1**	0	**+2**	**-1**	**-1**	+2	**-1**	**+3**	**+2**	+2
	Information Management	10	The organization tells me it will look after my personal information properly	0	**-5**	+1	-1	**-4**	+2	-1	+2	**+2**	**+4**
	Information Management	11[b]	The organization will completely delete all the information it holds about me when I ask it to	+1	**+2**	**-3**	+1	**+3**	+1	-1	0	**+3**	**+2**
	Information Security	12	The organization appears to have effective security processes to safeguard my personal information	+2	0	**+5**	**+5**	**-1**	**-1**	+1	+3	0	+1
	Information Security	13	The organization will tell me immediately if it gets hacked, or loses my personal information	**+4**	+3	**+1**	+2	+2	**0**	**+1**	+2	+3	**+5**
Technology Lens	Information Use	14	The technology service will tell me if it is tracking my behavior or location	**+3**	**+3**	-1	-1	-1	**-3**	**-2**	-1	+2	**+3**
	Information Use	15	The technology service will only collect personal information which is relevant	0	0	0	**+2**	**+1**	0	**-4**	**-1**	-1	+1
	Information Use	16	The technology service will allow me to check which items of my personal information it is collecting and using, and why	**+2**	**+2**	+1	0	**+2**	**-3**	**-2**	-1	+1	-1
	Information Principles	17	Although I may not get all the benefits, the technology service will not ask for lots of personal information before it allows me to use it	0	**+1**	-1	**+1**	**+2**	**+1**	0	**-3**	**-4**	-1
	Information Principles	18	The technology service will assume I don't want share my personal information, until I explicitly tell it to do so	**+2**	+1	**0**	**0**	+1	**+3**	**0**	+1	**0**	+2
	Information Principles	19	The technology service will not ask me for information I consider sensitive (e.g. income, relationship status, age etc.)	**+4**	+1	+2	**+2**	-2	**-2**	**-3**	**-2**	-1	0
	Information Management	20	The technology service will allow me to control who can see items of my personal information, and what they can see	**+5**	**+4**	**+1**	**+1**	+4	+2	+2	**+4**	**+1**	+2
	Information Management	21	The technology service will allow me to opt-in or opt-out all or parts of it, and see which parts I am enrolled into	**+3**	**+2**	**-2**	-1	**+3**	**-2**	**-2**	-1	+2	**-2**
	Information Security	22	The technology service uses security mechanisms (e.g. user name and password, or a "padlock" icon in the browser)	+2	**0**	+3	**+3**	**0**	**0**	+3	**0**	**+4**	**+3**
	Information Security	23[b]	The technology's security measures are approved by organizations who I trust (e.g. regulatory authorities)	+1	-1	**+2**	**+3**	**-3**	**-2**	**-3**	+1	0	+2
Other Factors	Consequences for Individual	24	Using the technology service will not affect my security, or the security of my family and friends (e.g. its use won't lead to stalking or burglary)	+3	**+5**	**+4**	+3	+2	+2	**+1**	**+5**	**+1**	**+1**
	Consequences for Individual	25	Using the technology service will not impact me financially (e.g. increased insurance costs, loss of credit status, running costs etc.)	**+1**	**+1**	**+1**	**+4**	**+4**	+3	**+4**	+2	+3	+3
	Protection	26	When I use the technology service I believe I will be protected by the law	-1	**+2**	**+4**	**+2**	**-2**	**0**	0	**+2**	+1	**0**
	Protection	27	I believe will be reimbursed if I lose money when using the technology service	+1	**-1**	**-1**	**+4**	+1	**+4**	0	0	**+5**	0
	Technology Features	28	The technology service looks like it will be easy for me to use	**-3**	-1	-2	-2	+1	**0**	**+2**	-2	-1	**-5**
	Technology Features	29	The technology service looks well-designed, robust and professional	**-2**	0	0	**-2**	0	**+4**	**+2**	0	0	0
	Technology Features	30	The technology service looks exciting and innovative	**-4**	-2	-3	**-3**	-2	**+3**	**+1**	-2	-2	**-3**
	Technology Features	31	The technology service looks like it will work well with other technologies or services I use (e.g. social networking works well on my mobile phone)	-2	**-1**	**-4**	**-5**	**-1**	**-1**	-3	-2	**-1**	-3
	Environmental Cues	32	I have not heard anything bad in the media about the organization or the technology service	-1	-2	**-3**	-2	-1	**-4**	**+3**	**+3**	**-3**	-2
	Environmental Cues	33	Lots of people use the technology service and they don't seem to have any problems	**-2**	-2	**-2**	**+1**	0	-2	**+5**	**+1**	0	**-3**
	Environmental Cues	34	Other technology services (e.g. Facebook, supermarket loyalty cards etc.) already collect my personal information	-3	-3	**-5**	**-4**	-3	**-1**	**-1**	**-4**	-3	-2
	Environmental Cues	35	I have done my own research on the organization and technology service and it seems okay	-1	0	-4	**-4**	-2	-1	**0**	**+1**	**-5**	-1
	Environmental Cues	36	My relatives, friends or work colleagues tell me it is okay to use the technology service	-2	**-3**	-1	**-3**	0	**0**	**+4**	**0**	**-3**	**-3**
	Benefits for Individual	37	The benefits offered by the technology service are useful to me	-1	+3	+2	**-1**	**+5**	**+5**	+3	+2	**-2**	**-1**
	Benefits for Individual	38	The technology service will use my personal information to help me (e.g. save me time and money, help me with my social life etc.)	**-3**	**-3**	0	**-3**	**+3**	**-3**	+2	**-3**	-2	**-4**
	Benefits for Individual	39	I can't get the same benefits offered by the technology service anywhere else	**-5**	**+2**	0	**-3**	**+3**	-2	-4	**-3**	-4	0
	Benefits for Individual	40	The technology service allows me to decide where, when and how I can use the benefits it provides	0	+1	**-2**	0	**+1**	**+3**	**-2**	-3	-1	**-4**

a. Factor scores in bold are those which are highest or equal highest (shaded dark gray) and lowest or equal lowest (shaded light gray) in their cohort. Sub-categories which are the principal focus of each group have a solid border.

b. Statements not based on specific coded quotations in the transcripts from earlier focus group study [10], but created specifically for the Q methodology study and based on discussions in the focus groups relating to the category.

TABLE V. COMPOSITION AND ALIGNMENT OF FACTORS IN EACH GROUP

Group Name	Eigenvalue	% of Variance Explained	Eigenvalue	% of Variance Explained	No. Significantly Loading Into Group (N=40)[c]	No. of Males	No. of Females	CPBOG (N = 28)[e]	DFP (N = 28)[e]
Information	Factor 1 (offline)		Factor 4 (online)					(n = 9)	(n = 9)
Controllers	4.92	16%	2.78	10%	10 (25%[d])	4	6	μ = 3.79; σ= 0.86	μ = 3.41; σ= 1.15
Security	Factor 2 (offline)		Factor 1 (online)					(n = 8)	(n = 8)
Concerned	2.89	9%	2.97	11%	10 (25%[d])	5	5	μ = 3.14; σ= 0.62	μ = 3.72; σ= 0.91
Benefit	Factor 3 (offline)		Factor 5 (online)					(n = 5)	(n = 5)
Seekers	2.56	8%	1.76	7%	8 (20%[d])	3	5	μ = 2.75; σ= 0.40	μ = 2.88; σ= 0.48
Crowd	Factor 4 (offline)		Factor 2 (online)					(n = 3)	(n = 3)
Followers	2.07	7%	2.37	9%	6 (15%[d])	3	3	μ = 4.33; σ= 0.92	μ = 2.72; σ= 1.39
Organizational	Factor 5 (offline)		Factor 3 (online)					(n = 3)	(n = 3)
Assurance Seekers	2.00	6%	2.86	11%	6 (15%[d])	1	5	μ = 3.51; σ= 0.18	μ = 2.56; σ= 0.84

[c] N = 40 as this is the number of participants who loaded significantly into only **one** group (i.e. excluding the one participant who negatively loaded significantly into Factor 4 (offline)).

[d] Percentages calculated as number of participants significantly loading into this group only, divided by total number of participants with only one significant positive loading (N = 40).

[e] N = 28, as 20 participants from the offline cohort and 8 from the online cohort completed the DFP and CPBOG measurement instruments [14] **and** loaded significantly into only one group. The CPBOG and DFP scores were calculated as the weighted average of the three items in the scales.

V. IDENTIFIED VIEWPOINTS (FACTOR NARRATIVES)

A. Information Controllers

The ability to control the collection, use and dissemination of personal information – using mechanisms provided by a technology lens – is very important for this group[11]. This echoes the results of a qualitative study by Olivero & Lunt [9], who found that e-commerce customers want instruments that provide them with active control over their information, allowing them to make informed decisions about trading their personal information for benefits.

This group's principal focus is who has access to their personal information and what they can see (20). The desire to control the flow of personal information accounts for why this group: a) want to know if their behavior or location is being monitored (14); b) value the ability to opt-in or opt-out of aspects of a technology service (21); c) do not like their personal information shared with others unless they have given their permission (18); and d) want to be able to monitor which items of personal information are being collected (16). They also prefer organizations which inform them if their personal information is repurposed (7), or shared with other parties (6). They may also be reluctant to provide information they consider sensitive (19*[12]), which may explain their focus on information control.

The importance this group attaches to controlling access to their personal information may be because of their anxiety about its potential effect on their personal security (e.g. stalking, burglary, etc.) (24*). A comment from one participant (ON.20)[13] in this group illustrates this concern:

> *"This appears to be the most crucial aspect, as safeguarding oneself and one's close ones seems most fundamental and a higher priority than using a new technology service, however useful it may be."*

However, this group is not particularly concerned about the possible financial impact of using a technology service (e.g. increased health insurance costs as a result of data collected about unhealthy lifestyles) (25). If they do experience problems, it is not clear if this group expect to be protected by the law (26*), and they are not too concerned whether an organization follows applicable laws and regulations (9). This may be because they prefer to take control of their personal information, rather than rely – *post priori* – on external protection and redress mechanisms.

Even with their preference for technical controls to manage personal information, this group does seek some reassurance from the providing organization. Because of their desire to control their personal information, they want an organization to inform them if a technology service suffers a security breach or loses their personal information (13). A participant (OFF.7) in this group remarked:

> "*In the event important information* […] *fall*[s] *into the wrong hands, there is potentially a great threat to the things I am part of. Stopping it at that stage and notifying me would allow me time to change my password and if need be, cancel/deactivate my card to prevent fraud attempts.*"

Environmental cues – such as the advice of friends and family (36), media stories (32), or that others already use a technology service (33) – do not influence this group. As one participant (OFF.30) observed:

> "*Other people may use the technology service without any problem but I am not sure who will be the next target of fraud or identity theft, so I am not really concerned about people using technology without any problem.*"

This group also does not readily accept that a technology service can collect personal information simply because others (e.g. social networking, supermarket loyalty cards, etc.) already do so (34).

This group are also unlikely to be impressed by organizations' claims concerning their safeguarding of personal information (4*, 5*, 10*), perceived competence (3*), size (2*) or reputation (1). They are more likely to rely

[11] Factor 1 (offline) ranked six of the eight statements categorized as *Technology Lens* (excluding *Information Security*) higher than the other factors in its cohort; the other two statements were ranked 0 (neutral). Factor 4 (online) ranked five of the statements higher, with the other three ranked 0 (neutral) or +1.

[12] References to Q-set statements where the offline and online cohorts did **not** rank the same statement: a) highest in their cohort; b) lowest in their cohort; c) neutral or ±1; d) higher than +1 and within one position; or e) lower than -1 and within one position, are indicated with an asterisk.

[13] Exemplar quotes are from participants who only loaded significantly into the group described in the factor narrative.

upon their ability to control personal information, rather than organizations' assurances. As one participant (OFF.13) noted:

> "[O]*rganizations and technological services are not always reliable, even when they state that they would not share any of my personal information online. I feel that the best way to go about doing this is to adopt a self-regulatory attitude towards the services. I feel more assured if I know I can control what I want and not want to share with others.*"

The features of a technology service – its ease of use (28*) and design (29*) – are likely to be of little interest to this group. They are not impressed by a technology just because it is innovative or exciting to others (30*). They also do not attach any significant importance to benefits, such as recommendations or personalization (38). However, it is not clear if this group is concerned about not being able to get the benefits offered by a technology service elsewhere (39*), or the usefulness of the benefits (37*).

B. Security Concerned

Security of personal information is of paramount importance to this group[14], exemplified by a participant (ON.10) who stated, "*Security is a critical element of the service*". This group also values technical security protections, such as the HTTPS padlock (22). This emphasis on information security is likely to be because of their anxiety about the detrimental effects using a technology service might have on their personal security (24), and possibly their finances (25*). This group's focus on security may also account for their preference for technology services from organizations – irrespective of the providing organization's size (2*) and competence (3*) – with sound information principles[15], a good reputation (1), and approved by, or linked with, organizations they trust, such as regulatory authorities or payment providers (23). As one participant (ON.37) observed, "*I trust the regulatory authorities* […] [to] *give me the best protection."*

Despite the focus on security, this group may not necessarily expect to be informed if an organization suffers a security breach (13). If a problem occurs, this group considers their legal protection to be very important (26), with a participant (OFF.1) stating "*I feel safer knowing I will be protected by the law if anything untoward happens* […]*".* Their desire for legal protection may explain why they are the only group who are likely to take an interest in the terms and conditions of using a technology service (8).

This group do not particularly like to be asked for information they consider to be sensitive (19) or irrelevant (15*), and definitely do not accept that because other technology services already collect, process and store information, new technology services should be allowed to do the same (34). This is part of a wider disregard of environmental cues by this group, including media reports (e.g. stories about hacking) (32), relatives or friends' advice (36*), and the wider population already using a technology service – apparently without problems (33*). As one participant (OFF.22) observed, "*I would need more validation than 'lots of people' as I would want actual authority backup* […]*".* Despite not relying on environmental cues, this group is unlikely to carry out their own research before using a technology service (35). The difficulty of determining the trustworthiness of new technology services was identified by a participant (ON.1) who noted:

> *"Many providers of new services are innovative start-ups and I would not necessarily expect to have heard of them. I don't have time to conduct research on all of the companies I come across on the internet* […]."

The features of a technology service, its ease of use (28), or design (29*), and whether it is innovative or exciting to others (30), is of little interest to this group. They are unconcerned about whether it will work well with other technologies they already use (e.g. a social networking website working well on a smartphone and PC) (31), with a participant (ON.10) remarking, "*I am not looking for integration of services – security is more important.*"

The lack of interest in technology may be why this group does not attach great importance to technical means of controlling their personal information (20, 18). They are keen for the providing organization to assume this responsibility, keeping them informed about the use to which their personal information is being put (7), why their personal information is being collected (4*), and who it is being shared with (6*). However, they may not expect an organization to delete their personal information when requested (11*).

Finally, this group is not particularly interested in the benefits provided by a technology service (37*) even if they cannot get the same benefits elsewhere (39*). Technology services that use personal information to provide targeted benefits, such as special offers or recommendations, are also unlikely to be sought (38*).

C. Benefit Seekers

Technology services that provide useful benefits are valued by this group – as long as they are not constrained in terms of where they can use them (e.g. discount vouchers). The principal focus of this group is best characterized by a participant (ON.30) who remarked:

> "*My main reason for using technology services is some sort of personal benefit, so most of all I consider whether it will be convenient for me* [or] *add convenience to my life.*"

Despite their focus on the benefits offered by a technology service, this group is concerned about the potential financial consequences of using it, and want to be reimbursed if they lose money. As well as benefits, this group considers its functionality to be important, suggesting it possibly has two principal foci – benefits *and* technology.

Perhaps unsurprisingly, this group is not too concerned about being asked for information they consider to be

[14] Factor 2 (offline) and Factor 1 (online) ranked effective organizational information security processes (12) as the most important (+5) statement. In addition to an organization's security processes, Factor 1 ranked three of the four statements in the two *Information Security* sub-categories higher than the other factors in its cohort, whilst Factor 2 ranked two of the statements higher.

[15] Factor 2 (offline) ranked both statements categorized as *Organization* (*Information Principles*) higher than the other factors in its cohort; Factor 1 (online) ranked one of the two statements higher.

sensitive. Assurances by organizations about stewardship of personal information are also of little interest – with one participant (OFF.12) declaring:

> "*Almost every organization would tell me that they will look after my information properly, and that makes no difference.*"

The lack of interest in organizations' assurances may explain why this group does not particularly value technology services which are approved by, or linked with, organizations they trust. The size of the organization providing the technology service, and its perceived competence are also likely to be of little interest to this group, although they do consider its reputation as being slightly important.

This group does not consider it at all important to read a technology service's terms and conditions. However, this should be regarded in light of the relative rankings of statement 8 – concerning the readability of a technology service's terms and conditions – which were less than -1 for all groups in both cohorts. Although the Q-methodology study only captured *intended* behavior; the low ranking of statement 8 is consistent with existing studies [23].

This group's low opinion of organizations' assurances about their privacy behavior may be because they like to have control of their information (e.g. who has access to personal information and what they can see), be kept informed about information being shared with third parties, and expect an organization to delete personal information when requested.

This group does not particularly seek out advice concerning a technology service from family or friends, and are not induced to use a technology service, simply because lots of other people may already be using it. They also do not readily accept that a technology service can collect personal information purely because others already do so; as one participant (ON.30) noted, "*Just because other services collect my information I don't automatically want others to have my information*", but admitted, "*when signing up for services I hardly ever consider what other technology services have* [access to] *my information.*"

Finally, although the sample size is small, and any conclusions can only be tentative, the mean CPBOG [14] for this group ($\mu = 2.75$; $\sigma = 0.40$; $n = 5$) is the lowest of the five groups (Table V).

D. Crowd Followers

Use of a technology service by others, the reputation of the organization providing the technology service, and the advice of family and friends are very important to this group. This is best illustrated by a participant (OFF.15) who admitted:

> "*I usually choose what technology service to use based on relatives and close friends' opinions. They are people I can trust so I believe they will give me an honest review."*

Innovative technology services which look professional, robust and easy to use are likely to be preferred by this group, with one participant (ON.35) observing, "*I like to be using* [...] *innovative products and services. I will always have a look and try anything new that sparks my interest.*"

It is therefore not clear from the factor analysis and comparison if this group might be better represented as two separate, overlapping, groups, both influenced by environmental cues, but with one attaching more importance to the features of a technology service.

This group may seek environmental cues for reassurance because they like innovative technology services, but are also concerned about the possible impact on personal security and costs. Their level of comfort with new technology may also explain their lack of concern about the collection of irrelevant or sensitive personal information.

E. Organizational Assurance Seekers

The assurances of organizations – possibly provided as privacy policies – about personal information collection, use and sharing makes this group comfortable to use a technology service. This is exemplified by a participant (ON.28) in this group who noted:

> "*A written disclaimer stating that it will look after my personal information imbues trust in the organization – if they go against it, then I have their word that says otherwise.*"

This group also looks for other forms of assurance. Information security is important for this group. Not only do they seek out technological security mechanisms (e.g. the HTTPS padlock symbol), but if an organization is not able to deliver against its assurances (e.g. its systems are hacked, or it loses information) they expect the organization to inform them immediately. This may possibly be because of their concern about the potential consequences of a breach.

Environmental cues, such as media reports, the advice of family and friends, and widespread use of a technology service do not greatly influence this group. This may be because this group trusts organizational assurances more than media reports. As one participant (OFF.18) remarked, "*I think some media organizations have stakes in certain services so I am reluctant to trust their opinion regarding technology*." This group is also not focused on the benefits provided by a technology service, nor its features.

Finally, although the sample size is small, the mean CPBOG [14] for this group ($\mu = 4.33$; $\sigma = 0.92$; $n = 3$) is the highest of the five groups (Table V). This may be because *Crowd Followers* seek reassurance from others to lessen their own privacy concerns.

VI. Discussion

Our study used Q methodology – an empirical research method for eliciting peoples' viewpoints, which has not yet been used in privacy research – to investigate if salient groupings of people could be found, based on the types of information cues they seek to minimize their concerns about using a technology service, and the perceived risks of disclosing personal information to it. Our results show that 40 of the 58 study participants (69%) could be segmented into one of five groups: 1) *Information Controllers* (25%) – who value individual control of the collection and dissemination of their personal information; 2) *Security Concerned* (25%) – who are principally concerned about their own security and

that of their personal information; 3) *Benefit Seekers* (20%) – who focus on the benefits offered by a technology service; 4) *Crowd Followers* (15%) – who follow the actions and advice of others; and 5) *Organizational Assurance Seekers* (15%) – who look for organizations' assurances about how they safeguard personal information entrusted to them. Of the remaining 18 participants, 11 (19%) could be placed into more than one group, and 7 (12%) could not be placed into any group. These latter participants may be represented by a group not identified by this study.

Practitioners can use the five-group segmentation to inform the construction of default privacy personas. For example, a social networking site could allow users to set their privacy preferences to "*follow the privacy settings of like-minded people*". However, our study shows that control over the disclosure of information – usually implemented as privacy preferences – is the principal focus of only 25% of study participants. The remainder prioritized cues relating to organizations' privacy behavior (*Security Concerned* and *Organizational Assurance Seekers*), and the behavior and advice of others (*Crowd Followers*). This latter group – who represent 15% of participants in the study – are influenced by information coming from the environment, of which *trust symptoms* [4] – difficult for organizations to forge or manipulate – are a significant component.

We suggest the findings from our study can assist practitioners in implementing the Seven Foundational Principles of Privacy by Design (PbD) [24]. In particular, recognition of the different information-seeking preferences of users can help practitioners meet the 7th PbD principle – *respect for user privacy*. By understanding what is important to different types of users, practitioners can ensure their technology services address users' privacy expectations.

The offline and online Q-sorts were undertaken approximately 6-8 months apart. There is the potential therefore for external events (e.g. media stories about hacking) to have influenced the two cohorts differently. However, we suggest that any proposed segmentation of users will need to be largely immune to such effects.

Our study did not investigate if the lack, or inadequacy of information cues sought by an individual raises their level of privacy concern, and hence their reluctance to adopt a technology service – this is the focus of future work. Nevertheless, our results suggest a more holistic approach to modeling privacy concern is required, which encompasses peoples' perceptions of the technology lens *and* information receiver components of a technology service [1]. Privacy research has largely focused on the efficacy of various privacy controls and preferences. Even the most usable of privacy-protecting mechanisms cannot mitigate an *Organizational Assurance Seeker's* distrust of an organization who offers little or no information in their privacy policy, or a *Crowd Follower's* disquiet that none of their friends have used a particular technology service.

REFERENCES

[1] A. Morton and M. A. Sasse, "Privacy is a process, not a PET: a theory for effective privacy practice," in *Proceedings of the 2012 workshop on New security paradigms*, New York, NY, USA, 2012, pp. 87–104.

[2] A. Adams and M. A. Sasse, "Privacy in Multimedia Communications: Protecting Users, Not Just Data," in *Human-Computer Interaction*, 2001.

[3] A. Adams and M. A. Sasse, "Privacy Issues in Ubiquitous Multimedia Environments: Wake sleeping dogs, or let them lie?," in *IFIP Conference on Human-Computer Interaction*, 1999.

[4] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy, "The Mechanics of Trust: A Framework for Research and Design," *Int. J. Hum.-Comput. Stud.*, vol. 62, no. 3, pp. 381–422, 2005.

[5] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: measuring individuals' concerns about organizational practices," *MIS Q.*, pp. 167–196, 1996.

[6] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Inf. Syst. Res.*, vol. 15, no. 4, pp. 336–355, Dec. 2004.

[7] S. Preibusch, "Guide to measuring privacy concern: Review of survey and observational instruments," *Int. J. Hum.-Comput. Stud.*, vol. 71, no. 12, pp. 1133–1143, Dec. 2013.

[8] A. Beldad, M. de Jong, and M. Steehouder, "A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet," *Inf. Soc.*, vol. 27, no. 4, pp. 220–232, 2011.

[9] N. Olivero and P. Lunt, "Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control," *J. Econ. Psychol.*, vol. 25, no. 2, pp. 243–262, Apr. 2004.

[10] A. Morton, "'All my mates have got it, so it must be okay': Constructing a Richer Understanding of Privacy Concerns - An Exploratory Focus Group Study," in *Computers, Privacy and Data Protection: Reloading Data Protection*, S. Gutwirth and R. Leenes, Eds. Springer, 2014.

[11] W. Stephenson, *The study of behavior; Q-technique and its methodology*. Chicago, Illinois: University of Chicago Press, 1953.

[12] M. J. Culnan and R. J. Bies, "Consumer privacy: Balancing economic and justice considerations," *J. Soc. Issues*, vol. 59, no. 2, pp. 323–342, 2003.

[13] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Secur. Priv. Mag.*, vol. 3, no. 1, pp. 26–33, Jan. 2005.

[14] A. Morton, "Measuring Inherent Privacy Concern and Desire for Privacy - A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern," in *2013 International Conference on Social Computing (SocialCom)*, 2013, pp. 468–477.

[15] D. H. McKnight and N. L. Chervany, "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology," *Int. J. Electron. Commer.*, vol. 6, no. 2, pp. 35–59, 2001.

[16] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An Integrative Model of Organizational Trust," *Acad. Manage. Rev.*, vol. 20,, no. 3, pp. 709–734, Jul. 1995.

[17] J. Van Exel and G. de Graaf, "Q methodology: A sneak preview." 2005.

[18] K. O'Leary, J. O. Wobbrock, and E. A. Riskin, "Q-methodology As a Research and Design Tool for HCI," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2013, pp. 1941–1950.

[19] P. M. ten Klooster, M. Visser, and M. D. T. de Jong, "Comparing two image research instruments: The Q-sort method versus the Likert attitude questionnaire," *Food Qual. Prefer.*, vol. 19, no. 5, pp. 511–518, Jul. 2008.

[20] T. Webler, S. Danielson, and S. Tuler, "Using Q method to reveal social perspectives in environmental research," *Greenfield MA Soc. Environ. Res. Inst.*, Feb. 2009.

[21] S. R. Brown, "Q Methodological Tutorial," *QUALRS-L@UGA (University of Georgia)*, 1992-1991. [Online]. Available: http://facstaff.uww.edu/cottlec/QArchive/Primer1.html. [Accessed: 16-Apr-2013].

[22] S. Watts and P. Stenner, *Doing Q Methodological Research: Theory, Method & Interpretation*. Los Angeles, CA: Sage Publications, 2012.

[23] T. Vila, R. Greenstadt, and D. Molnar, "Why we can't be bothered to read privacy policies models of privacy economics as a lemons market," *Proc. 5th Int. Conf. Electron. Commer.*, pp. 403–407, 2003.

[24] A. Cavoukian, "Privacy by Design - The 7 Foundational Principles," Office of the Information and Privacy Commissioner, Ontario, Jan. 2011.