Routledge
Taylor & Francis Group

Journal of Risk Research

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rjrr20

E-privacy concerns: a facet theoretical approach

Gisela Böhm, Hans-Rüdiger Pfister, Vanessa Ayres-Pereira & Ingvar Tjøstheim

JOURNAL OF RISK RESEARCH
https://doi.org/10.1080/13669877.2023.2288012

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

E-privacy concerns: a facet theoretical approach

Gisela Böhm[a,b], Hans-Rüdiger Pfister[c,*], Vanessa Ayres-Pereira[a] and Ingvar Tjøstheim[d]

[a]Department of Psychosocial Science, University of Bergen, Bergen, Norway; [b]Department of Psychology, Inland Norway University of Applied Sciences, Lillehammer, Norway; [c]Institute for Experimental Industrial Psychology (Luenelab), Leuphana University Lüneburg, Germany; [d]Norwegian Computing Center, Oslo, Norway

ABSTRACT

Although the ubiquitous use of smartphones and social media poses serious risks to the privacy of users, research is sparse regarding how users perceive these risks. We present a study investigating the perception of e-privacy risks, assuming that risk perception depends on context and situation, and employing a facet theory approach to define and analyze privacy risk perceptions. Specifically, we define three facets that characterize situations involving an e-privacy risk: Facet A refers to the type of data disclosed, distinguishing three types: a person's identity information, information about health, and information about private activities. Facet B refers to the type of actor misusing the information, distinguishing between commercial organizations, public authorities, social networks, and criminal actors. Facet C distinguishes three kinds of harm that might be experienced as a consequence: financial loss, physical harm, and negative psycho-social experiences. Questionnaire items were constructed by creating fictitious but realistic scenarios, each representing a combination of one element from each facet, yielding 36 (3×4 × 3) scenarios. For each scenario, respondents rated the likelihood and the negativity of experiencing that scenario. Following the facet theoretical paradigm, item intercorrelations were analyzed *via* ordinal multidimensional scaling. Results from a representative survey among 500 adult Norwegians yield a distinct partitioning with respect to Facets A and B, called a radex configuration. Facet B (actors) shows an angular partition. Facet C (type of harm) yields a contrast of financial versus psycho-social harm. In sum, we conclude that our three-faceted definition provides a satisfying first approximation to people's perception of privacy risks on the Internet while remaining open for extensions with additional facets.

ARTICLE HISTORY
Received 19 March 2023
Accepted 22 November 2023

KEYWORDS
E-privacy; facet theory; risk perception; social media; data protection

Introduction

The ubiquitous use of the internet and of social media services has enabled individuals, companies, and public authorities to generate, store, process, and distribute personal data to an extent previously unknown. Such massive handling of personal data has made concerns about violations and abuse of private data a major research area (Acquisti, Brandimarte, and Loewenstein 2015) and a central topic for empirical studies in diverse domains and from different disciplinary

CONTACT Gisela Böhm gisela.boehm@uib.no Department of Psychosocial Science, University of Bergen, Bergen, Norway.

*Present address: Department of Psychosocial Science, University of Bergen, Bergen, Norway.

perspectives (Bhatia and Breaux 2018; Dinev and Hart 2006; Gana and Koce 2016; Sætra 2020; Shahidi et al. 2022; Shariff, Green, and Jettinghoff 2021; Smith, Milberg, and Burke 1996).

Privacy has a long cultural history (Aries, Duby, and Veyne 1987; Westin 1967), and the concept of privacy in its modern sense has been studied by scholars from various backgrounds and applied to a diverse range of social life areas (Burgoon 1982; Nissenbaum 2010; Sætra 2020; Solove 2008; Stone et al. 1983; Zuboff 2015). A common premise of these different conceptions is that privacy is something to be protected. Threats to privacy may encompass physical privacy (e.g. overcrowded prisons), social privacy (e.g. traditional families), and information privacy. Information privacy can be defined as one's ability to control others' access to any piece of information about oneself, from one's address to one's sexual preferences (Bélanger and Crossler 2011). We specifically focus on information privacy as related to information available on the internet, primarily information distributed *via* the use of social media (SNS: Social Network Sites) such as Facebook, WhatsApp, and the like, but also *via* public administration websites, medical management sites, e-commerce platforms, and many others. We use the term *e-privacy* or ePrivacy (European Commission 2017), referring to privacy issues involving any digital data and communication system, particularly internet platforms and SNS as described above.

E-privacy can be thwarted and violated in many ways, ranging from abuse within social media to unauthorized usage for commercial purposes, to criminal cases such as identity theft and hacker attacks. Furthermore, in the digital economy, personal data have monetary value, and some argue that one should consider data a form of payment when using digital services (Elvy 2017). Many users may not be aware of this function of personal data, or if they are, they may not fully understand the complexity of data use and be unable to grasp the implications of trading private data for some kind of benefit (Nissenbaum 2019). Sætra (2020) argues that privacy is an aggregate public good and cannot be addressed individualistically. Nissenbaum (2011, 2019) emphasizes that what counts as private data and what may or may not be made publicly available strongly depends on the context of data exchange. Depending on the context, different rules and norms apply when dealing with confidential information. For example, in a health context, people commonly trust their doctor and are willing to provide personal data, whereas in a business context, very different norms govern the transmission of information. We will draw on this contextual approach when defining relevant facets of situations involving threats to privacy. We are interested in which factors influence people's concern about privacy issues, especially concerns about the potential misuse of private information.

It seems obvious that people should be concerned about privacy issues and interested in keeping relevant information private and confidential while being fully informed and in full control of who may access their personal data. A so called *privacy paradox* has been observed in several studies, showing a gap between expressed concerns and actual behavior. In other words, when asked, people express a substantial degree of concern about and willingness to protect their data, but they mostly do not behave in a way that effectively protects their privacy (Acquisti, Brandimarte, and Loewenstein 2015; Ayres-Pereira et al. 2022; Brandimarte Acquisti, and Loewenstein 2013; Kokolakis 2017; Spiekermann, Grossklags, and Berendt 2001). It has been argued that the paradox disappears when the relation between attitudes and behavior is analyzed within an appropriate framework such as the theory of planned behavior (Dienlin and Trepte 2015), and when intention and behavior are matched with respect to specificity. A specific situation implies information about aspects such as type of confidential data, type of possible misuse, etc. Thus, people might be concerned about privacy in some situations but oblivious about privacy in others, depending on the context (Nissenbaum 2010, 2019).

One reason for this inconclusive research evidence might be the lack of an appropriate theoretical definition of e-privacy that is sufficiently detailed to derive concrete situations and application contexts. Most attempts to define e-privacy derive from Westin's (1967) definition, which emphasizes the right of individuals "… to determine for themselves when, how, and to what extent information about them is communicated to others". This general definition, with its focus on individual control, might be too vague to be applied to the multitude of online contexts (Nissenbaum 2010, 2019; see also Solove 2008). Nissenbaum (2010, 2019) in particular argues that online privacy is not fundamentally different from traditional privacy; the crucial distinction is not between the online and non-online domain but between different contexts, such as health/medicine, or friends/relatives, each with its own special rules and norms that regulate what should be kept private and confidential and what can be disclosed without concern.

This theoretical deficiency is also reflected in existing instruments measuring e-privacy. E-privacy concerns have been assessed predominantly *via* self-report scales (Bhatia and Breaux 2018; Buchanan et al. 2007). A problem in the literature is that, despite the construct's relevance, a common unifying framework for measuring it does not seem to have emerged yet. The scales that have been developed vary in terms of scope and dimensions. While some scales assess privacy concerns on a very general level (Hong and Thong 2013; Malhotra, Kim, and Agarwal 2004; Mwesiumo et al. 2021; Smith, Milberg, and Burke 1996; Stewart and Segars 2002), others focus on perceptions specific to particular devices or technical applications such as apps (Buck, Burster, and Eymann 2018). The number of dimensions also varies by study. For instance, whereas some scales identified dimensions such as concerns about data collections, errors, unauthorized access, and secondary use (Smith, Milberg, and Burke 1996; Stewart and Segars 2002), others focus on control factors and awareness of privacy practices (Malhotra, Kim, and Agarwal 2004). A recent review compared survey methods used to measure e-privacy concerns in experimental studies that examine causal relationships between e-privacy concerns and data disclosure decisions (Matre, Englund, and Ayres-Pereira 2021). The authors found that most of the studies analyzed used adapted versions of published scales, with wide variations in the number of items and content. Considering the multifaceted and context-dependent nature of the concept, it is relevant to develop measurement instruments whose items cover the multiple facets that potentially influence risk perceptions. In other words, surveys attempting to measure privacy concerns should address the different aspects and components about which people may be concerned and specify the specific context of application (Nissenbaum 2011). According to the review of Matre, Englund, and Ayres-Pereira (2021), although most of the analyzed items measuring privacy concerns inquired about the actions of some agent upon the users' data, less than half of them specified who the agent was. Those items that specified the agent referred to companies in general (social network sites, websites, and e-commerce) or individuals (referred to as "people", "others" or "somebody"). Besides, only about a quarter of the items described which type of data was processed, and it was usually worded as abstract "personal information" or "personal data". Also, the items rarely specified the type of personal negative consequences that could arise from data disclosure.

A noteworthy advancement in the field is the work of Bhatia and Breaux (2018), who studied people's willingness to share private information as a function of several contextual factors such as data purpose, data type, likelihood of privacy violations, and presumed benefit of sharing private data. Specifically, Bhatia and Breaux (2018) constructed vignettes describing a situation in which a person might share private information on the internet by systematically combining different levels of the contextual factors. It was thus possible to identify under which conditions people are more willing to share information and when people are more likely to avoid sharing their private data.

Given the lack of an appropriately detailed theoretical definition of e-privacy and the resultant variability in e-privacy measurement instruments, our study aims to explore e-privacy risk perceptions. We assume that risk perception in the context of e-privacy depends on situational factors; we employ a facet theory approach (Guttman and Greenbaum 1998) to define and analyze these perceptions. In contrast to studies like Bhatia and Breaux (2018) that rely on regression models to predict privacy-related behavior, our primary goal is to determine the semantic structure of content facets by systematically varying the composition of relevant situations according to the facet elements (Shye 2014, 2015).

Along these lines, we propose that e-privacy concerns refer to, or are respectively triggered by, specific situations and specific contexts. Rather than constituting a generic disposition of individuals to be more or less concerned about privacy in a broad sense or expressing a dispositional risk attitude towards privacy abuse, we assume that e-privacy concerns depend on the specific situational context involving four interconnected entities (Figure 1). We conceive of an *e-privacy situation for concern* as a connected structure in which some *person* using the internet makes *data* available (voluntarily or involuntarily), which can be obtained by some *actor*, who may subsequently cause some kind of *harm* to this person using the data in question. For example, a person using social media provides information about health issues to his or her online friends, which is used by a pharmacy company to sell ineffectual medication to that person, causing financial loss and possibly physical harm. Thus, the degree of concern a person experiences may depend on the genuine connection between personal data, particular actor(s), and subsequent harm.

A faceted definition of e-privacy concerns

Based on pertinent work (Acquisti, Brandimarte, and Loewenstein 2015; Bhatia and Breaux 2018; Dogruel and Joeckel 2019; Gstrein and Beaulieu 2022; Milne et al. 2017; Nissenbaum 2019; Schomakers et al. 2019), and derived from the situation model outlined above (Figure 1), we propose a faceted definition of e-privacy situations for concern with three facets: Type of data, type of actor, and type of harmful consequences. With this definition and the subsequent analyses, we follow a facet-theoretical approach as originally developed by Guttman (1954); for further advances and applications, see Borg and Shye (1995), Canter (1985), Guttman and Greenbaum (1998), Hackett (2021), Levy (2014), Shye (2015), or Solomon (2022). Facet theory provides a methodological framework that allows us to establish theoretical constructs that can be reliably based on empirical regularities. The theoretical framework is formulated as a so called mapping sentence (Figure 2), which defines the essential semantic-logical structure of the construct under study (the 'facets') and serves as a blueprint for constructing samples of specific items for empirical measurement.

Quantitative assessments of items constructed as systematic combinations of facet elements are correlated and subjected to ordinal Multidimensional Scaling (Borg and Groenen 2005). Regional patterns are then identified in the obtained multidimensional geometric space that correspond to the faceted definition (Cohen, 2014), Levy (2014), and Shye (2015) describe typical

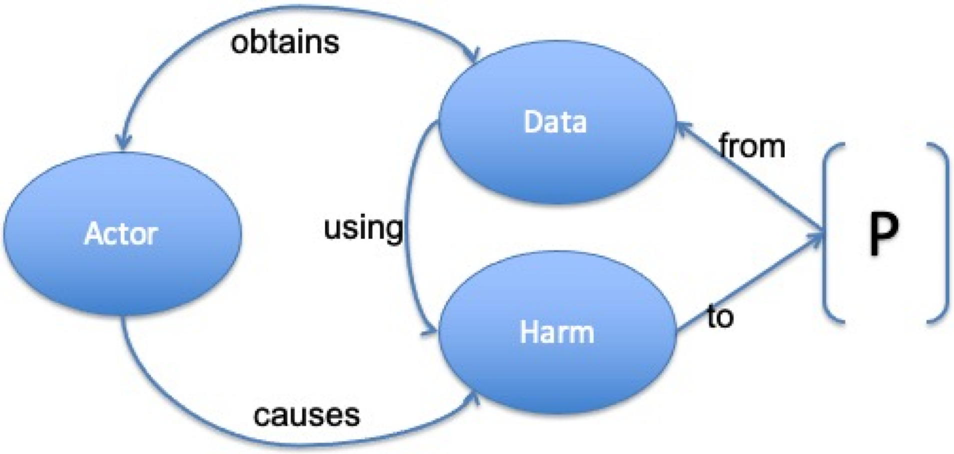

Figure 1. Elements and connections of an e-privacy situation of concern.

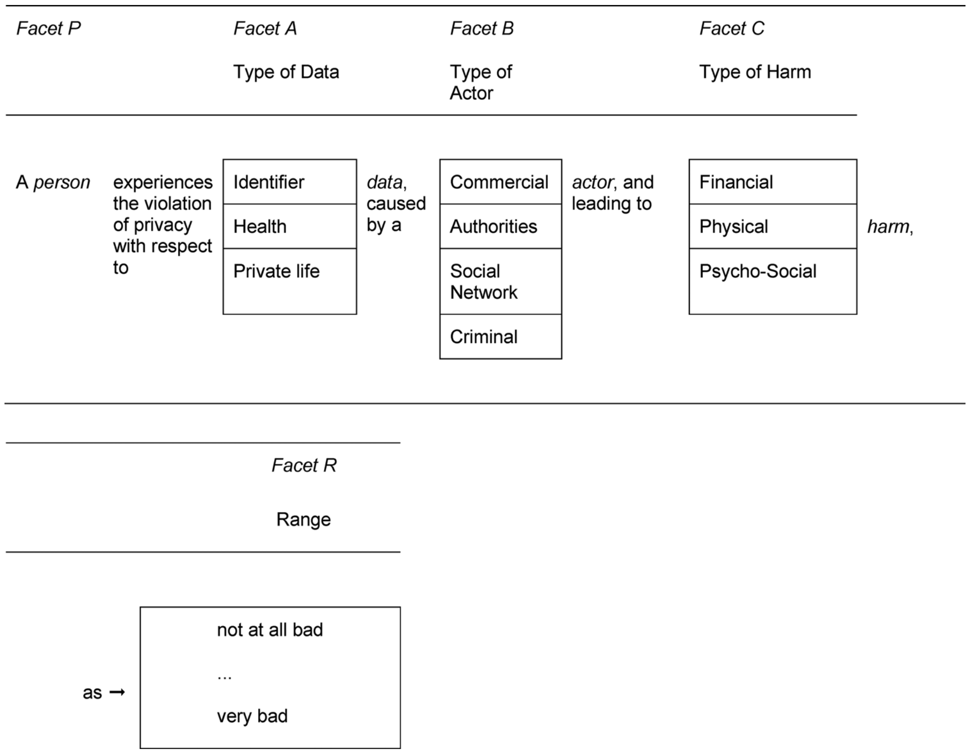

Figure 2. Mapping sentence.

patterns such as simplex, circumplex, and radex. If such a correspondence between the faceted definition of a construct and empirical patterns of items derived from the mapping sentence can be determined, the construct is regarded as representing a meaningful empirical regularity; in other words, it is maintained that facets are semantic distinctions that capture relevant empirical regularities. Examples come from intelligence research (Guttman and Levy, 1991), cultural studies (Ginges and Cairns 2000), quality of life research (Borg 1978), and environmental psychology (Böhm et al. 2019; Böhm et al. 2020); for a synopsis, see Shye (2015).

We suggest a faceted definition of e-privacy situations for concern comprising three facets: type of data, type of actor, and type of harm; consisting of three, four, and three elements, respectively.

Facet A refers to the *Type of Data* involved in the scenario. This facet consists of three elements: identifiers, health data, and data about one's private life. For example, identifiers can include credit card numbers or IP addresses, health data may encompass medical histories or data from body sensors, and private life data could involve sexual preferences or family problems communicated *via* social media networks.

We define data type as the kind of data in question; we refer to data that a person considers to be private and over which they demand control in terms of who may access these data and how the data may be used. As Nissenbaum (2011, 2019) argues, what people consider private and are willing to share is to a great extent context-dependent. For example, in the context of a medical consultation, people may agree to giving information about health issues to their doctor and implicitly assume confidentiality. Similarly, if a person voluntarily shares family photos publicly on Instagram, the pictures are no longer private, and the person does not see them as strictly private data that can be misused by others. However, it is still possible that a third party accesses these photos illegitimately and thus creates a situation of concern. In our study, we focus on situations for concern and explicitly consider situations of data misuse.

Similar to our study, Bhatia and Breaux (2018) included data type as a factor. They used data type to predict willingness to share and found significant effects in two studies. Data type was implemented as a mixed collection of specific information items, such as credit card number, home address, password, etc.; however, these items were not classified into superordinate categories as we did. In a related comprehensive study, Schomakers et al. (2019) report findings about people's sensitivity to 40 different data types. They found high sensitivities for identifying information and medical data and medium sensitivity for private information, such as sexual preferences or political affiliation. Notably, each and every of the 40 data types can be clearly mapped to one of our three elements of Facet A.

Facet B refers to the *Type of Actor* responsible for privacy violations. We distinguish four elements: a commercial actor (e.g. an online company), a public or governmental authority (e.g. a labor office), a member of one's social network (e.g. friends on Facebook), or a criminal (e.g. a hacker). This categorization is supported by a study by Dogruel and Joeckel (2019), who analyzed privacy risk perceptions and found four major domains perceived as risky and prone to privacy violations: governmental, criminal, commercial, and social. Nissenbaum (2019) also recognizes relevant actors, such as the recipient of confidential information, as core elements of the context that demarcate the norms and expectations of information transmission.

Facet C refers to the *Type of Harm* caused by privacy abuse. We distinguish three kinds of harm: financial loss (e.g. unauthorized purchases), physical harm (e.g. taking harmful medication), or psycho-social harm (e.g. social harassment causing psychological distress due to the disclosure of sexual or political preferences). There is limited research on the impact of negative consequences on privacy concerns. In one of the rare studies, Milne et al. (2017) investigated consumers' risk perceptions of personal data sharing and identified four risk categories: physical, psychological, monetary, and social. These correspond to our Facet C elements, only that we combined psychological and social into one facet element, 'psycho-social' harm. Privacy harm is also one of the factors used by Bhatia and Breaux (2018) to predict willingness to share information; examples of harms used in their scenarios were surveillance, induced disclosure, or appropriation. Although analogous to our harm categories, Bhatia and Breaux (2018) focus on unintended consequences of sharing private information (e.g. surveillance or disclosure), whereas we focus on subjectively experienced personal losses or detriments (e.g. harassment as a result of disclosure).

Method

Item construction and response scale

The mapping sentence defines three content facets: data, actor, and harm. The person facet defines the person experiencing the situation as an individual randomly selected from some population, and the range facet defines the common meaning under which corresponding situations are evaluated. The combination (the Cartesian product) of the three content facets yields 3 (data) × 4 (actor) × 3 (harm) = 36 types of situations. For example, a situation in which a criminal (actor) uses an identifier (data), which causes psychological distress (harm) for the person. Such a combination is called a structuple (Shye 1998) and can be viewed as an abstract depiction of a situation for concern. A particular instance of a structuple is then a description of a concrete scenario with the facet elements specified. Theoretically, the number of conceivable instances for a structuple is unlimited, and each specific set of items is just a sample from the universe of possible items. For each of the 36 structuples derived from the mapping sentence, one concrete scenario was constructed (see Appendix), yielding 36 items representing 36 specific scenarios of e-privacy violations.

Participants rated each item on two eleven-point scales: a *likelihood* scale ("How likely do you think it is that this happens to you?") ranging from 0 (not likely at all) to 10 (very likely), and a *negativity* scale ("How negative would it be if this happened to you?") ranging from 0 (not at all negative) to 10 (very negative); we presume a priori that such a situation cannot be experienced as positive.

Sample and data collection

A representative sample of 502 participants, drawn from a Norwegian panel, responded to all 36 items (in randomized order), as well as a few additional demographic questions. Of the participants, 51.2% were female, 48.8% were male, and the mean age was 48 years.

Data collection was carried out by the commercial research company YouGov and was based on their Norwegian online panel.

Analysis

First, we report results concerning differences between the mean ratings for the elements of each facet, pointing out differences and indicating those elements that cause the most concern. Since we have no pre-specified hypotheses, these findings are mainly descriptive.

Second, we focus on our main research question and report the results from various multidimensional scaling analyses based on item correlations; we examine the configurations of items highlighting the kind of regional patterns that could (or could not) be identified with respect to the faceted definition.

We restrict our analyses to the negativity ratings because the likelihood ratings were all quite low and yielded no structural regularities. Obviously, the majority of participants considered all scenarios as rather unlikely. Also, likelihood judgments have been proven to be notoriously difficult in the literature (Morewedge and Kahneman 2010; Reyna 2004), and attempts to construct psychologically sound likelihood measurements are preliminary at best (Bhatia and Breaux 2018).

Mean differences

Table 1 shows the means of each facet element for all three facets. The overall mean of negativity ratings across all 36 items is $M = 6.53$ ($SD = 3.31$). For Facet A, a situation involving an identifier as data type is rated as most negative; for Facet B, a situation involving a criminal as an actor is rated as the most negative; and for Facet C, physical harm is rated as the most negative type of harm. Descriptively, the differences appear rather small. A repeated measurement analysis of variance with the three facets as independent variables yields significant main effects as well as significant interactions (Table 2). Pairwise post-hoc comparisons show that only Health

Table 1. Means of negativity ratings of facet elements for each facet.

Facet A Type of data	Identifier	Health	Private Life	
	6.74	6.44	6.40	
Facet B Type of actor	Commercial	Authorities	Social network	Criminal
	5.93	6.81	6.31	7.06
Facet C Type of harm	Financial	Physical	Psycho-social	
	6.50	6.85	6.23	

Note. Each facet element mean is computed as the average across all other facets.

Table 2. Repeated measurement ANOVA with negativity rating as dependent variable.

Effect	num.Df	den.Df	MSE	*F*	η2, *p*η^2	*p*-value
Facet A	1.945	974.462	6.292	32.971	.002, .062	0.000
Facet B	2.827	1,416.554	8.047	152.451	.018, .233	0.000
Facet C	1.918	961.010	8.200	74.776	.006, .130	0.000
A:B	5.828	2,919.680	5.096	33.349	.005, .062	0.000
A:C	3.812	1,909.587	5.042	24.970	.003, .047	0.000
B:C	5.728	2,869.850	4.890	31.359	.005, .059	0.000
A:B:C	10.944	5,482.856	5.301	49.691	.015, .090	0.000

Note. Degrees of freedom (Df) are Greenhouse-Geisser corrected; effect sizes are eta-squared (η^2) and partial eta-squared (*p*η^2).

and Private Life do not differ significantly (Facet A), whereas all other comparisons yield significant differences ($p < .01$, Tukey adjustment for multiple comparisons). Effect sizes are very small, with Facet B (Type of Actor) yielding the largest effect (partial eta-squared is .233).

Structural analyses

As mentioned earlier, we do not use the likelihood ratings. All structural analyses are thus based on the negativity ratings only. The likelihood scale turned out to have very low mean values, small variances, and uninterpretable covariances; the vast majority of respondents judged the scenarios as very unlikely.

As a measure of similarity, we used the product-moment correlation coefficient. Using a non-metric coefficient such as Guttman's monotonicity coefficient μ (Guttman 1986) yields virtually identical results.

Item-level MDS analysis

A distance matrix was constructed based on the correlations between all 36 items. The correlation r_{ij} between two items i and j was converted to a dissimilarity d_{ij} according to $d_{ij} = \sqrt{1-r_{ij}}$. The complete dissimilarity matrix was submitted to ordinal multidimensional scaling (Borg and Groenen 2005; Mair, Groenen, and De Leeuw 2022), and a two-dimensional configuration was used for interpretation. Goodness-of-fit is acceptable (*Stress-1*=0.203), and a permutation test (Mair, Borg, and Rusch 2016) yields a median stress value of S=0.327. A one-sided test with μ = .01 yields a critical value of 0.308, indicating that the observed stress value is significantly smaller than would be expected for random data.

With 36 items, regional patterns for facet elements are difficult to detect in a two-dimensional plane. For this reason, and for the sake of parsimony, we do not show the configuration based on all 36 items. To obtain a more succinct and less noisy result, we perform a series of MDS analyses on aggregated structuples with a focus on two facets at a time, averaging across the remaining third facet; this yields three analyses showing the partial structure of Facets A and B, of B and C, and of A and C, respectively.

Facets A and B: type of data and actors

Structuples resulting from the combination of Facet A and Facet B, aggregated across Facet C, denote the combination of the Type of Data facet and the Actor facet, resulting in 3×4=12 variables. Note that these structuples do not represent concrete situations but correspond to abstract situation types, constructed by averaging across the three elements of Facet C (Type of Harm). Computation of the dissimilarity matrix was done as described above; an ordinal MDS yields a two-dimensional configuration with *Stress*=0.122 (significantly smaller than the critical value of 0.142, μ = .01, according to a permutation test). Figure 3 shows the configuration with a superimposed radex pattern.

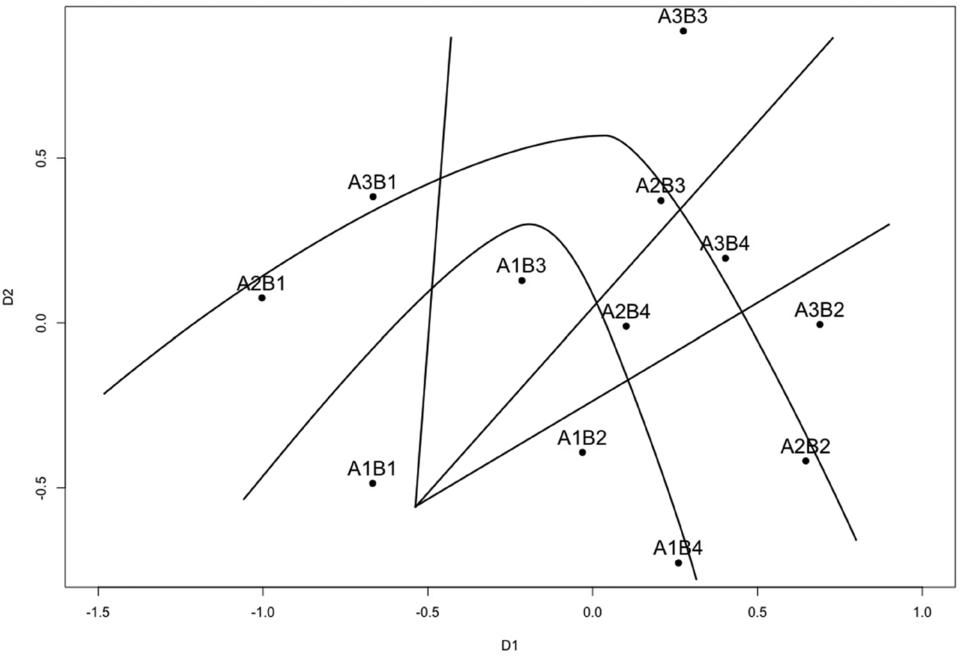

Figure 3. Two-dimensional configuration of twelve structuples representing Facets A and B, aggregated across Facet C. Stress = 0.122. Regional separation lines (radex) superimposed (for structuple descriptions see the mapping sentence in Figure 2 and the complete wording of the items in the Appendix).

With respect to Facet A, the configuration can be partitioned into three circular layers: Identifier data (A1) located in a central region, health data (A2) located in an intermediate region, and private life data (A3) located in the periphery. Facets corresponding to this kind of circular regionality are called radial facets (Shye 2015).

A different pattern emerges with respect to Facet B. Its elements can be separated by straight lines, forming wedge-like regions originating from a common origin. From left to right, we find commercial actors (B1), social network actors (B3), criminal actors (B4), and authorities (B2). Facets forming this kind of circularly ordered sectors are called angular facets; superimposing a radial and an angular facet yields a radex configuration (Guttman 1954). With respect to Facet B, there is one deviating structuple A1B4 (identifier-criminal) located in the lower right.

Identifier data (A1) are located in the center, indicating high similarity among all A1 structuples. Health (A2) and private life (A3) data are less homogenous and more differentiated depending on Facet B (the type of actor involved). In particular, we may conjecture that health and private life, though separable, constitute a common region, with health forming a special sub-concept of private life. For Facet B (actors), the configuration implies that the actors are ordered: from commercial to social to criminal to authorities. We will consider possible explanations in the discussion section. To corroborate these empirical regularities, Figure 4 depicts, for each facet, the convex hull for each of its facet elements; for Facet A, the convex hulls show a nested structure typical for a radial facet, and for Facet B, the convex hulls are practically non-overlapping, confirming the angular pattern.

To summarize, we propose that the conceptual structure, as defined by Facets A (Type of Data) and B (Actors), could be sufficiently substantiated by regional patterns corresponding to facet elements in a regular fashion (Shye 1998, 2014, 2015). It should be noted that identifying regional patterns is different from a dimensional interpretation; regional patterns are invariant to rotations and translations of the coordinate system, and we thus do not attribute any

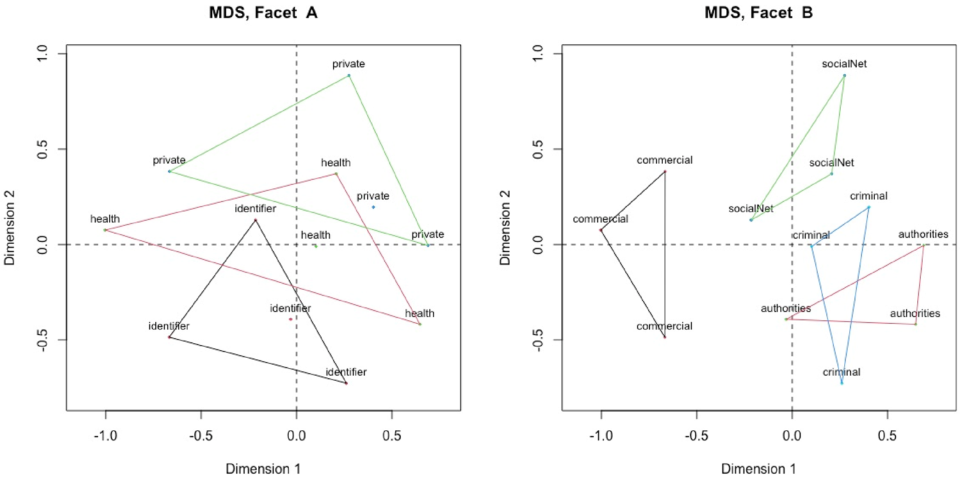

Figure 4. (a) Facet A elements with convex hulls; (b) Facet B elements with convex hulls.

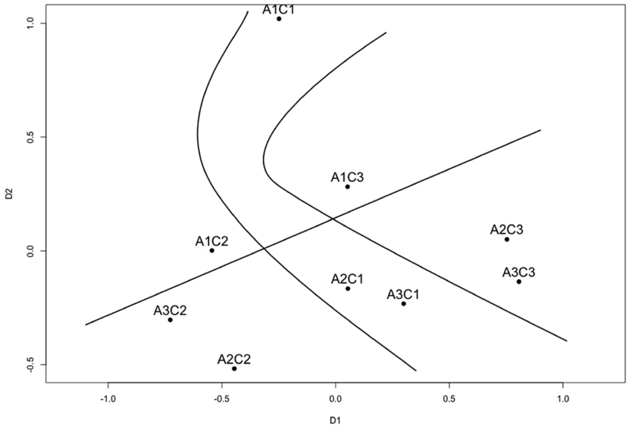

Figure 5. Two-dimensional configuration of nine structuples representing Facets A and C, aggregated across Facet B. Stress = 0.073. Regional separation lines (radex) superimposed (for structuple descriptions see the mapping sentence in Figure 2 and the complete wording of the items in the Appendix).

intrinsic meaning to the two dimensions; they are used merely as auxiliary axes to embed the configuration of structuples in Figures 3 and 4.

Facets A and C: type of data and type of harm

Aggregating across Facet B (Actors) generates nine structuples combining Facet A (Type of Data) and Facet C (Type of Harm). An ordinal MDS analysis on the dissimilarity matrix yields a two-dimensional configuration with *Stress* = 0.074, which falls within the 99% interval [0.023, 0.203] of stress values compatible with a random distribution (permutation test). This means that the stress value is not significantly lower than what would be expected for a random configuration. Yet, it is important to note that the number of structuples in this configuration is relatively low, so low stress values are to be expected even for random configurations.

We provide a regional separation in Figure 5, as well as the convex hulls of facet elements in Figure 6. Facet C, Type of Harm, can be clearly separated into radial regions, with C3 (psycho-social harm) as an inner region, C1 (financial harm) forming a small intermediate region, and C2 (physical harm) in the outer area.

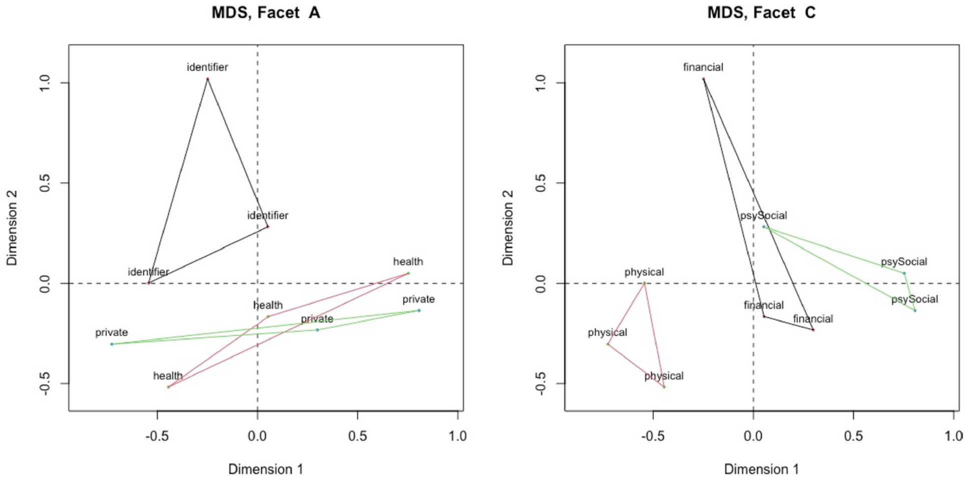

Figure 6. (a) Facet A elements with convex hulls; (b) Facet C elements with convex hulls.

With respect to Facet A, Type of Data, a separation is only possible by opposing A1 (identifier) from a common region containing A2 (health) and A3 (private life) structuples; this confirms the pattern observed in the analysis of the AB structuples that health data and private life data are closely connected. The convex hull representations in Figure 6 validate this partitioning. While the configuration is based on only nine points, we see the result as supportive of the conceptual validity of Facet C, and partly of Facet A.

Facets B and C: type of actor and type of harm

We proceed with Facets B (Type of Actor) and C (Type of Harm) in an equivalent way: The dissimilarity matrix of $4\times3=12$ structuples, after averaging across Facet A, was input to an ordinal MDS analysis, yielding a $Stress=0.136$ for the two-dimensional solution. This stress value is significantly lower, according to a permutation test, than the critical lower value of 0.151 (μ = .01), rejecting the null hypothesis of a random pattern.

For Facet B (actors), we find a clear separation for B1 (commercial), opposed to B3 (social network); in-between, the B2 (authorities) and B4 (criminal) elements are not separable (Figure 7). For Facet C (Type of Harm), the facet elements can be partitioned into a tripartite pattern, with C1 (financial harm) in an intermediate position, and C3 (psycho-social harm) and C2 (physical harm) located adjacently to the left and right, respectively.

The convex hull representation (Figure 8) highlights this regional pattern, being reminiscent of a circumplex going from physical to financial to psycho-social harm, possibly indicating an ordering from severely harmful to less harmful.

Table 3 provides a summary of the main results. Overall, we find supporting evidence for all facets, albeit with some restrictions. Concerning Facet A (Type of Data), it turns out that health and private life are not consistently separable as well-defined regions. Regarding Facet B (Type of Actor), results suggest that commercial and social network actors constitute distinct concepts, but authorities and criminal actors partly overlap and intersect with the other facet elements.

Discussion

Psychological research on e-privacy focuses on the following research questions: a) What determines people's perceptions of the risk of abuse of their personal data on the internet? b) What

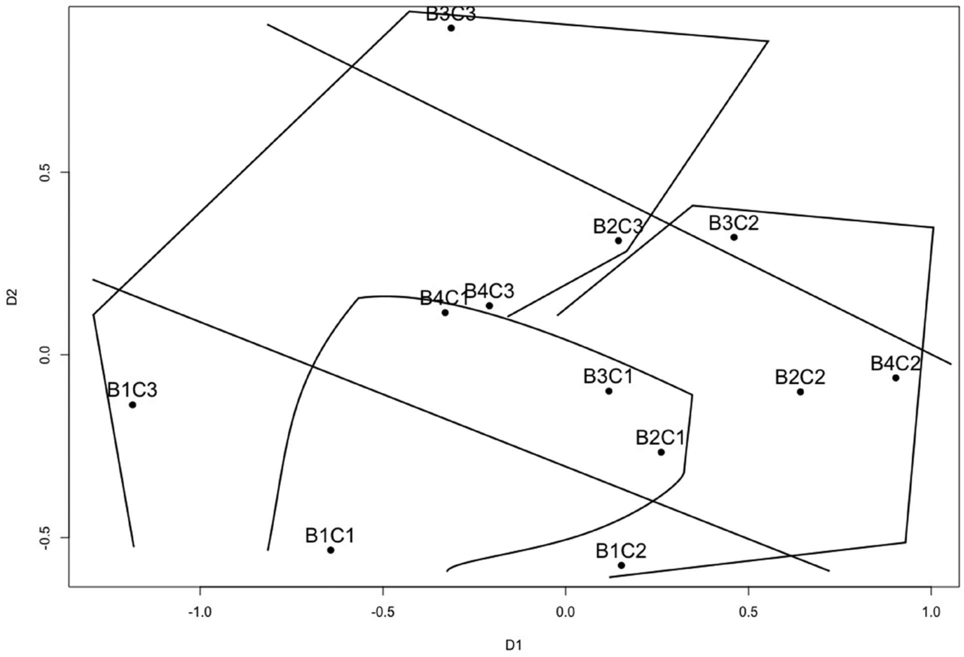

Figure 7. Two-dimensional configuration of twelve structuples representing Facets B and C, aggregated across Facet A. Stress = 0.136. Regional separation lines superimposed (see the mapping sentence in Figure 2, for the complete wording see the Appendix).

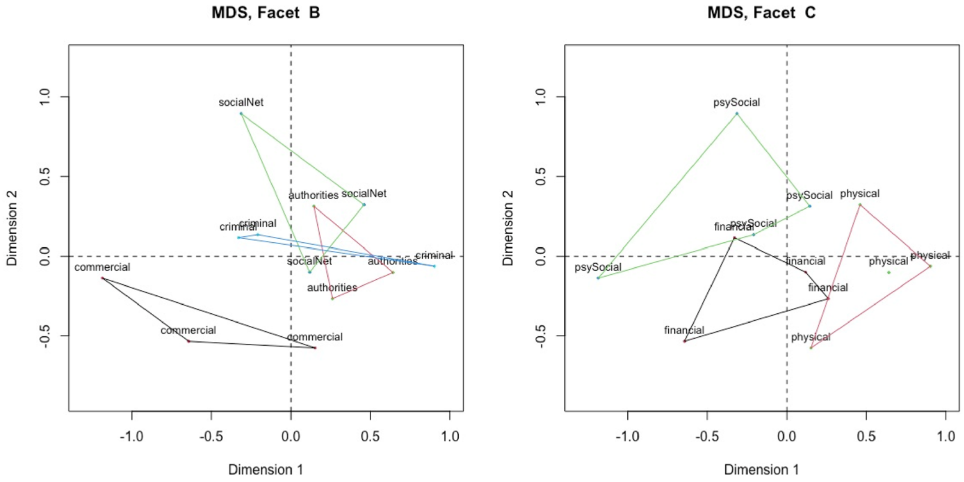

Figure 8. (a) Facet B elements with convex hulls; (b) Facet C elements with convex hulls.

Table 3. Summary of MDS analyses of aggregated structuples.

Analysis	*Facet A*	*Facet B*	*Facet C*	*Stress*
A and B	Confirmed	Confirmed		0.122*
A and C	Partially confirmed (health and private life inseparable)		Confirmed	0.073 n.s.
B and C		Partially confirmed (authorities and criminals inseparable)	Confirmed	0.136*

are the relevant factors of concern about violations of e-privacy? and c) How do people behave when they are concerned about their personal data? Previous research in this field has suffered from a lack of a theoretically coherent and empirically validated definition of e-privacy concern. Key studies toward such a definition include Nissenbaum (2011, 2019) and Bhatia and Breaux (2018). Using a facet theory approach, we propose an empirically supported contextual definition of e-privacy situations for concern. That is, we propose a definition of what constitutes an e-privacy situation for concern for internet users and present empirical evidence that provides support for this proposal. The definition is cast in the form of a mapping sentence, a core concept of facet theory. The mapping sentence we propose comprises three facets that we assume represent three major components of a situation for concern: The type of data involved in the situation, the type of actor who is responsible for the violation of e-privacy, and the type of harm caused by the violation. In facet theory, facets represent the essential categorical distinctions of the phenomenon under study. The elements of a facet represent possible realizations of that category; here, the three elements of data type are identifier, health data, and private life information, the four elements of actor type are commercial, authorities, social network, and criminal, and the three elements of harm are financial, physical, and psycho-social harm.

The faceted definition serves as a template to construct scenario vignettes; combining all 3 × 4 × 3 elements yields 36 structuples, that is, possible types of situations. Each scenario constitutes an item and can be viewed as a concrete instance of a structuple. Each item was assessed by participants with respect to its perceived negativity and likelihood. On average, the scenarios were perceived as highly unlikely but very negative. Due to the consistently low likelihood ratings, we exclusively focused on negativity ratings in our analyses. Mean differences of facet elements in negativity are significant, but effect sizes are small. Following standard facet analysis, we focus on structural similarities between scenarios, that is, on item inter-correlations, rather than on mean differences. A series of ordinal multidimensional scaling analyses on the correlations between aggregated structuples yields largely confirming evidence for the proposed faceted definition. For each of the three facets, we find corresponding partitions in the MDS configurations (see Table 3), with very few misplacements and generally low stress values, indicating a good fit of the solutions.

Consistent segmentations can be identified for Facet A (Type of Data); specifically, a radial partition is obtained when analyzing aggregates of Facet A and Facet B (Type of Actor). Identifier data are located in the center, with health data and private data stratified towards the periphery. In combination with Facet B, which shows a clear angular partition, a typical radex structure is obtained. A radial partitioning is also found for Facet C, with financial harm in the central region and physical and psycho-social harm forming more outer segments. We interpret these findings as strong support for the validity of the three-faceted definition of e-privacy situations with respect to people's concern about violations.

However, there are a few misplacements of specific elements that suggest modifications of the definition and, consequently, the mapping sentence. Concerning Facet A, health and private life data are not consistently separated. It seems plausible that people's perception of health data is, in fact, such that they are an intrinsic part of their private life, indistinguishable from other personal information concerning the negativity of misuse. For further research, we suggest a simplification of this facet, involving only two elements: formal identifiers and information about one's private life, including health issues.

A more surprising finding is the non-separability of two elements of Facet B (Type of Actor): authorities and criminals. Possibly, infringements of e-privacy by authorities and criminal actors trigger the same preconceptions of social trust. Norway is generally a country with high social trust, and trust in the government is also generally high (Schmidthuber, Ingrams, and Hilgers 2021; Stein, Buck, and Bjørnå 2021). Criminal activities may thus collide with people's default expectation that fellow human beings are basically trustworthy; public authorities and administrations are considered prominently trustworthy, so even minor irregularities in administrative procedures may strongly disappoint citizens' beliefs. While criminals and authorities may be similar in this respect, we do not propose to fuse public administration and criminals into one element, as they are obviously qualitatively different in other respects, such as legitimacy. A theoretical effort is needed to reformulate the relevant elements that make up the category of actors in the context of e-privacy violations. One possibility is to introduce a further facet, namely, distinguishing between the actors themselves, and adding a facet that specifies the actor's intention. This new facet could distinguish whether the misuse of the data and resulting harm to the person is intended by the actor or not. The facet might consist of two elements, distinguishing wicked and vicious intentions, as they are arguably typical for criminals, from negligence and thoughtlessness, which might arguably be more applicable to public servants or members of one's social network. A related extension would be to include expected benefit as an additional facet (Bhatia and Breaux 2018), as the intended use of personal data typically conveys whether any benefits can be expected for the person.

A major advantage of facet theory is that it naturally lends itself to theoretical modifications and improvements, as well as empirical replications. Based on the current empirical findings, facets can and should be added (or removed), and facet elements reconsidered. Possible candidates include factors such as risk likelihood and data purpose, as studied by Bhatia and Breaux (2018), who found significant effects on willingness to share one's private data depending on the indicated likelihood of privacy misuse and the purpose of collecting private data, for example, to counteract terrorism. However, we want to emphasize that unlike Bhatia and Breaux (2018) or other studies based on regression models to predict privacy-related behavior, we are interested in determining the semantic-logical structure of content facets that constitute situations of concern. That is, our aim is to define and empirically validate the aspects that are psychologically relevant aspects of e-privacy situations. Following Nissenbaum's theory of contextual integrity (Nissenbaum 2010, 2019), we postulate that privacy behavior is largely controlled by contextual factors and rules, and that these factors are systematically structured and rooted in psychological processes of judgement and evaluation.

The facet theory approach, and in particular the mapping sentence, allows for genuine cumulative scientific progress (Guttman and Greenbaum 1998; Hackett 2021; Shye 2015). Generally, replication attempts can take two forms: The Person facet usually refers to a random sample from some population, and it is, in principle, easy to replicate with another random sample or with another prespecified population, using the same items. Another form of replication refers to the items representing the structuples. As outlined above, a structuple, say, A1B1C1 (a commercial actor misuses identifier data and causes financial harm), serves as a template to construct concrete scenarios, where the elements are specified in a way that generates a plausible concrete situation. Thus, each set of scenarios is just a sample from the theoretically infinite universe of structuple instantiations, and a replication using a different and new set of scenarios constitutes a straightforward and rigorous test of the faceted definition. Both lines of replication are fruitful and beneficial for cumulative research.

Disclosure statement

The authors report there are no competing interests to declare.

Ethics statement

The study was registered in the university system of risk and compliance in the processing of personal data in research projects (RETTE). The methods were acknowledged by the Norwegian Center for Research Data (NSD; notification form 695287). The patients/participants provided their informed consent to participate in this study.

Funding

This work was supported by the Norwegian Research Council under Grant 270969.

Data availability statement

The data that support the findings of this study are available from the corresponding author, GB, upon reasonable request.

References

Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221): 509–514. https://doi.org/10.1126/science.aaa1465

Aries, P., Duby, G., & Veyne, P. (Eds.). 1987. *A History of Private Life*. Vol. 1–5. Cambridge, MA: Cambridge University Press.

Ayres-Pereira, V., A. Pirrone, M. Korbmacher, I. Tjøstheim, and G. Böhm. 2022. "The Privacy and Control Paradoxes in the Context of Smartphone Apps." *Frontiers in Computer Science* 4: 986138. https://doi.org/10.3389/fcomp.2022.986138

Bélanger, F., and Crossler, R. E. 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* 35 (4): 1017–1041. https://doi.org/10.2307/41409971

Bhatia, J., and T. D. Breaux. 2018. "Empirical Measurement of Perceived Privacy Risk." *ACM Transactions on Computer-Human Interaction* 25 (6): 1–47. https://doi.org/10.1145/3267808

Böhm, G., R. Doran, A. Rødeseike, and H.-R. Pfister. 2019. "Pathways to Energy Transition: A Faceted Taxonomy." *International Studies of Management & Organization* 49 (3): 303–319. https://doi.org/10.1080/00208825.2019.1623981

Böhm, G., R. Doran, D. Hanss, and H.-R. Pfister. 2020. "Pathways to Energy Transition: Replication of a Faceted Taxonomy." *Umweltpsychologie* 24 (1): 153–161.

Borg, I. 1978. "A Comparison of Different Studies of Quality of Life." In *Zeitschrift für Sozialpsychologie* 9(2): 152–164.

Borg, I., and P. J. F. Groenen. 2005. "Modern Multidimensional Scaling." *Theory and Applications*. 2nd ed. New York: Springer.

Borg, I., and S. Shye. 1995. *Facet Theory: Form and Content*. Vol. 5. Thousand Oaks, CA: Sage Publications.

Brandimarte, L., A. Acquisti, and G. Loewenstein. 2013. "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4 (3): 340–347. https://doi.org/10.1177/1948550612455931

Buchanan, T., C. Paine, A. N. Joinson, and U. D. Reips. 2007. "Development of Measures of Online Privacy Concern and Protection for Use on the Internet." *Journal of the American Society for Information Science and Technology* 58 (2): 157–165. https://doi.org/10.1002/asi.20459

Buck, C., S. Burster, and T. Eymann. 2018. An Experiment Series on App Information Privacy Concerns. Paper presented at the 26th ECIS 2018: European Conference on Information Systems, Portsmouth, UK.

Burgoon, J. K. 1982. "Privacy and Communication." *Annals of the International Communication Association* 6 (1): 206–249. https://doi.org/10.1080/23808985.1982.11678499

Canter, D. (Ed.) 1985. *Facet Theory: Approaches to Social Research*. New York: Springer.

Cohen, E. H. Structural Hypotheses, In Encyclopedia of Quality of Life and Well-Being Research, edited by A. C. Michalos, 6383–6389. New York: Springer.

Dienlin, T., and S. Trepte. 2015. "Is the Privacy Paradox a Relic of the past? An in-Depth Analysis of Privacy Attitudes and Privacy Behaviors." *European Journal of Social Psychology* 45 (3): 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., and P. Hart. 2006. "An Extended Privacy Calculus Model for e-Commerce Transactions." *Information Systems Research* 17 (1): 61–80. https://doi.org/10.1287/isre.1060.0080

Dogruel, L., and S. Joeckel. 2019. "Risk Perception and Privacy Regulation Preferences from a Cross-Cultural Perspective. A Qualitative Study among German and US Smartphone Users." *International Journal of Communication* 13: 1764–1783.

Elvy, S.-A. 2017. "Paying for Privacy and the Personal Data Economy." *Columbia Law Review* 117 (6): 1369–1460.

European Commission. 2017. Proposal for a Regulation on Privacy and Electronic Communications. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications

Gana, M. A., and H. D. Koce. 2016. "Mobile Marketing: The Influence of Trust and Privacy Concerns on Consumers' Purchase Intention." *International Journal of Marketing Studies* 8 (2): 121. https://doi.org/10.5539/ijms.v8n2p121

Ginges, J., and D. Cairns. 2000. "Social Representations of Multiculturalism: A Faceted Analysis." *Journal of Applied Social Psychology* 30: 1345–1370. https://doi.org/10.1111/j.1559-1816.2000.tb02524.x

Gstrein, O. J., and A. Beaulieu. 2022. "How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches." *Philosophy & Technology* 35 (1): 3. https://doi.org/10.1007/s13347-022-00497-4

Guttman, Louis, and Shlomit Levy. 1991. "Two Structural Laws for Intelligence Tests." *Intelligence* 15 (1): 79–103. https://doi.org/10.1016/0160-2896(91)90023-7.

Guttman, L. 1954. "A New Approach to Factor Analysis: The Radex." In *Mathematical Thinking in the Social Sciences*, edited by P. F. Lazarsfeld, 258–348. New York: Free Press.

Guttman, L. 1986. "Coefficients of Polytonicity and Monotonicity." In *Encyclopedia of Statistical Sciences*, edited by S. Kotz and N. L. Johnson, 80–87. Vol. 7. New York: Wiley.

Guttman, R., and C. W. Greenbaum. 1998. "Facet Theory: Its Development and Current Status." *European Psychologist* 3 (1): 13–36. https://doi.org/10.1027//1016-9040.3.1.13

Hackett, P. M. W. 2021. *Facet Theory and the Mapping Sentence. Evolving Philosophy, Use and Declarative Applications*. 2nd ed. Basingstoke: Palgrave Macmillan.

Hong, W., and J. Y. L. Thong. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies." *MIS Quarterly* 37 (1): 275–298. Www.jstor.org/stable/43825946

Kokolakis, S. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64: 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Mair, P., I. Borg, and T. Rusch. 2016. "Goodness-of-Fit Assessment in Multidimensional Scaling and Unfolding." *Multivariate Behavioral Research* 51 (6): 772–789. https://doi.org/10.1080/00273171.2016.1235966

Mair, P., P. Groenen, and J. De Leeuw. 2022. "More on Multidimensional Scaling and Unfolding in R: smacof Version 2." *Journal of Statistical Software* 102 (10): 1–47. https://doi.org/10.18637/jss.v102.i10

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15 (4): 336–355. https://doi.org/10.1287/isre.1040.0032

Matre, A., M. Englund, and V. Ayres-Pereira. 2021. "Partial Results of a Review of Survey Methods Measuring e-Privacy Concerns." Paper presented at the 20th International Conference WWW/Internet and Applied Computing, Lisbon, Portugal.

Milne, G. R., G. Pettinico, F. M. Hajjat, and E. Markos. 2017. "Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing." *Journal of Consumer Affairs* 51 (1): 133–161. https://doi.org/10.1111/joca.12111

Morewedge, C. K., and D. Kahneman. 2010. "Associative Processes in Intuitive Judgment." *Trends in Cognitive Sciences* 14 (10): 435–440. https://doi.org/10.1016/j.tics.2010.07.004

Mwesiumo, D., N. Halpern, T. Budd, P. Suau-Sanchez, and S. Bråthen. 2021. "An Exploratory and Confirmatory Composite Analysis of a Scale for Measuring Privacy Concerns." *Journal of Business Research* 136: 63–75. https://doi.org/10.1016/j.jbusres.2021.07.027

Nissenbaum, H. 2010. *Privacy in Context*. Redwood City: Stanford University Press. https://doi.org/10.1515/9780804772891

Nissenbaum, H. 2011. "A Contextual Approach to Privacy Online." *Daedalus* 140 (4): 32–48. https://doi.org/10.1162/DAED_a_00113

Nissenbaum, H. 2019. "Contextual Integrity up and down the Data Food Chain." *Theoretical Inquiries in Law* 20 (1): 221–256. https://doi.org/10.1515/til-2019-0008

Reyna, V. F. 2004. "How People Make Decisions That Involve Risk – A Dual-Process Approach." *Current Directions in Psychological Science* 13 (2): 60–66. https://doi.org/10.1111/j.0963-7214.2004.00275.x

Sætra, H. S. 2020. "Privacy as an Aggregate Public Good." *Technology in Society* 63 (Nov 2020): 101422. https://doi.org/10.1016/j.techsoc.2020.101422

Schmidthuber, L., A. Ingrams, and D. Hilgers. 2021. "Government Openness and Public Trust: The Mediating Role of Democratic Capacity." *Public Administration Review* 81 (1): 91–109. https://doi.org/10.1111/puar.13298

Schomakers, E.-M., C. Lidynia, D. Müllmann, and M. Ziefle. 2019. "Internet Users' Perceptions of Information Sensitivity – Insights from Germany." *International Journal of Information Management* 46: 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Shahidi, N., V. Tossan, S. Bourliataux-Lajoinie, and S. Cacho-Elizondo. 2022. "Behavioural Intention to Use a Contact Tracing Application: The Case of StopCovid in France." *Journal of Retailing and Consumer Services* 68: 102998. https://doi.org/10.1016/j.jretconser.2022.102998

Shariff, A., J. Green, and W. Jettinghoff. 2021. "The Privacy Mismatch: Evolved Intuitions in a Digital World." *Current Directions in Psychological Science* 30 (2): 159–166. https://doi.org/10.1177/0963721421990355

Shye, S. 1998. "Modern Facet Theory: Content Design and Measurement in Behavioral Research." *European Journal of Psychological Assessment* 14 (2): 160–171. https://doi.org/10.1027/1015-5759.14.2.160

Shye, S. 2014. "Faceted Smallest Space Analysis (FSSA)." In *Encyclopedia of Quality of Life Research*, edited by A. Michalos, 2129–2133. New York: Springer.

Shye, S. 2015. "New Directions in Facet Theory." In *15th International Facet Theory Conference*, edited by S. Shye, E. Solomon, and I. Borg, 147–158. New York City: Fordham University.

Smith, H. J., S. J. Milberg, and S. J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly* 20 (2): 167–196. https://doi.org/10.2307/249477

Solomon, E. (Ed.) 2022. *Facet Theory in Organizational Research*. New York: Routledge.

Solove, D. J. 2008. *Understanding Privacy*. Cambridge MA: Harvard University Press.

Spiekermann, S., J. Grossklags, and B. Berendt. 2001. "*E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior*." Paper presented at the Proceedings of the 3rd ACM conference on Electronic Commerce.

Stein, J., M. Buck, and H. Bjørnå. 2021. "The Centre–Periphery Dimension and Trust in Politicians: The Case of Norway." *Territory, Politics, Governance* 9 (1): 37–55. https://doi.org/10.1080/21622671.2019.1624191

Stewart, K. A., and A. H. Segars. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument." *Information Systems Research* 13 (1): 36–49. https://doi.org/10.1287/isre.13.1.36.97

Stone, E. F., H. G. Gueutal, D. G. Gardner, and S. McClure. 1983. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations." *Journal of Applied Psychology* 68 (3): 459–468. https://doi.org/10.1037/0021-9010.68.3.459

Westin, A. F. 1967. *Privacy and Freedom*. New York: IG Publishing.

Zuboff, S. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89. https://doi.org/10.1057/jit.2015.5

Appendix.

List of 36 scenarios (structuples). Original text is in Norwegian, English translation added

Structuple	Norsk item text	English item text
A1B1C1	Du kjøper bøker fra en nettbokhandel, uten å være klar over at du har lagt igjen kredittkortinformasjon. Dette innebærer samtykke til deres 12-måneders bokklubbabonnement, som koster 250 kroner per måned.	You bought books from an online bookstore, unaware that you left your credit card information. This implied consenting to their 12-month book club subscription, which costs 250 kroners per month.
A1B1C2	Du legger inn adressen din i en treningsapp. Uten ditt samtykke sender bedriften deg en gratis forsyning av kosttilskudd. Du inntar tre av dem, som resulterer i kvalme og oppkast i tre dager.	You enter your address into a fitness app. Without your consent the company sends you a free supply of nutritional supplements. You consume three of them, and as a result you get nauseous and throw up for three days.
A1B1C3	Et reklamebyrå misbruker et nærbilde av deg i sin reklamekampanje. Du ønsket ikke dette og blir svært opprørt.	An advertising agency misuses a close up photograph of you in their ad-campaign. You did not want this and become very upset.
A1B2C1	Du laster ned en film ulovlig, politiet fanger opp IP-adressen din og bruker den til å spore adressen din. Du mottar en bot på 3000 kroner.	You illegally download a movie, the police collect your IP-address and tracks your address, and you receive a fine of 3000 kroner
A1B2C2	Et familiemedlem overfører penger til deg. NAV overvåker nettbanken din og registrer dette som inntekt som overskrider din rapporterte inntekt. Du mister din finansielle støtte og kan ikke lenger betale for en tannlege, som resulterer i dårlig tannhelse.	A family member transfers money to you. The Norwegian Labour and Welfare Administration (NAV) is monitoring your bank account and registers this as income that exceeds your reported income. You lose your financial support, and can no longer pay for a dentist, which results in poor dental health.
A1B2C3	Du kjøper ulovlig medisin på nett. IP-adressen din fra kjøpet blir fanget opp av politiet og de dukker opp på døren din for å gi deg en advarsel.	You purchase illegal medication online. Your IP-address from the purchase is collected by the police and they show up at your door to give you a warning.
A1B3C1	Du låner bort en strømmetjeneste til en venn. Vedkommende kjøper filmer for 500kr, og pengene blir trukket fra bankkontoen din.	You lend your friend your streaming account. They purchase movies for 500 kroners, and the money is deducted from your bank account.
A1B3C2	Du deler lokasjonen din i sosiale medier, som fører til at ekskjæresten din oppsøker deg. Vedkommende er agressiv, og du vrikker ankelen i det du løper fra stedet.	You share your location in social media, which leads to your former partner seeking you out. They are aggressive, and you sprain your ankle as you flee the scene.
A1B3C3	En venn tagger din geografiske lokasjon i et sosiale medier-innlegg som indikerer at du ikke er hjemme. Kollegaene og sjefen din ser dette og er sinte ettersom du har ringt inn syk. Ingen på jobb snakker med deg lenger.	A friend tags your location in a social media post, indicating that you're not home. Your boss and colleagues are furious since you called in sick. You experience being excluded at work.

Structuple	Norsk item text	English item text
A1B4C1	Du kjøper en smarttelefon på nett for 10 000 kroner med kredittkortet ditt. Nettbutikken viser seg å være svindel og du mottar aldri mobilen du bestilte eller pengene tilbake.	You buy a smartphone for 10 000 kroner online with your credit card. The shop turns out to be a fraud and you never receive the phone you ordered, nor do you get your money back.
A1B4C2	Du deler lokasjonen din i sosiale medier som indikerer at du er på ferie. En innbruddstyv ser dette og bryter seg inn i huset ditt. Du har kommet tidlig hjem fra ferien din og blir angrepet og skadet av tyven.	You share your location in social media, indicating that you are on vacation. A burglar sees this and breaks into your home. You have returned early from your vacation and you get assaulted and injured by the burglar.
A1B4C3	Basert på identifiserende informasjon som du har delt i din åpne sosiale medier-konto, lager noen en konto som utgir seg for å være deg. Du er desperat og vet ikke hva du skal gjøre med det.	Based on identifying information you shared through your open social media account, someone makes an account pretending to be you. You're desperate and don't know how to go about it.
A2B1C1	En treningsapp sporer din fysiologiske helsetilstand og anbefaler deg å kjøpe dyre kosttilskudd for å forbedre tilstanden din. Du kjøper kosttilskuddet, men det viser seg at tilstanden din ikke forbedrer seg, og pengene var bortkastet.	A fitness app keeps track of your physical health status and advises you to buy expensive dietary supplements to improve your health. You buy the nutritional supplements, but it turns out that your health does not improve, and the money was wasted.
A2B1C2	Treningsappen din indikerer at du er overvektig. Et nettapotek kjøper denne informasjonen og tilbyr deg slankepiller. Du tar pillene, og får alvorlig diare.	Your fitness app indicates that you are overweight. An online pharmacy buys this information and offers you weight loss pills. You take the pills, and you get severe diarrhea.
A2B1C3	Du kjenner en kul på halsen og søker det opp på en nettside. For å lese må du samtykke til informasjonskapsler. Senere får du opp reklame for kreftbehandling, som gjør at du stresser over kulen på halsen.	You feel a lump in your neck, and you look it up on a website. To read you must accept cookies. Later, you are shown advertisements for a cancer treatment, which contributes to you stressing over the lump.
A2B2C1	Helseinformasjonen din er lagret i din nettbaserte helsejournal. Basert på disse dataene erklærer helsevesenet, mot din vilje, at du ikke er i stand til å jobb. Dette resulterer i tap av inntekt.	Your health information is stored in your online medical journal. Against your will, the healthcare system classifies you as unable to work based on these data. This results in a loss of income.
A2B2C2	Din positive koronatest er registrert i din nettbaserte helsejournal. På grunn av dette nekter staten deg å forlate hjemmet ditt, noe som fører til at du ikke får gått til fysioterapeuten din og ryggsmertene dine forverres betydelig.	Your positive COVID-19 test is registered in your online health journal. Because of this, the government forbids you to leave your home, which leads to you missing an appointment with your physiotherapist and your back pains are amplified.
A2B2C3	Ved en feil sender helsevesenet testresultatet ditt for en seksuelt overførbar sykdom til alle i kommunen din. Du blir svært flau når du møter naboene dine.	The health care system mistakenly mails your test result for a sexually transmitted disease to everyone in your municipality. You feel very embarrassed when meeting your neighbours.
A2B3C1	I en meldingsapp forteller du en kollega om hvordan angstlidelsen din påvirker effektiviteten på hjemmekontor. Kollegaen din tar skjermbilde av samtalen og sender den til sjefen din, som resulterer i redusert stilling og lønn.	On a messenger app, you tell a colleague how your anxiety disorder affects your efficiency when working from home. Your co-worker screenshots the message and sends it to your boss, which results in a demotion and reduced salary.
A2B3C2	Du har en seksuelt overførbar sykdom. Ved et uhell deler vennen din dette på nett, som resulterer i at partneren din skader deg.	A friend accidently shares online that you have a sexually transmitted disease, resulting in your partner injuring you.
A2B3C3	Du forteller en venn at du/din partner er gravid, og vedkommende tagger deg i innlegg om graviditet i sosiale medier. Dette forårsaker mye spekulasjon blant venner og familie, noe som resulterer i stress.	You tell a friend that you/your partner are pregnant, who then tags you in posts about pregnancy in social media. This causes a lot of speculation amongst your friends and family, which results in stress.

Structuple	Norsk item text	English item text
A2B4C1	Din nettbaserte helsejournal blir hacket, og kriminelle truer med å dele informasjon som indikerer at du har en seksuelt overførbar sykdom dersom du ikke betaler 10 000 kroner. Du betaler.	Your online health journal is hacked, and criminals are threatening to share information indicating that you have a sexually transmitted disease unless you pay 10 000 kroner. You pay.
A2B4C2	En kriminell hacker legemiddelsystemet på nett, får tilgang til reseptene dine og henter ut medisinene dine. Dette resulterer i at du ikke får tatt medisinen din og du blir alvorlig syk.	A criminal who hacks the online prescription system and gets access to your prescriptions, collects your medication. As a result you are unable to take your medication and you become seriously ill.
A2B4C3	En kriminell hacker din nettbaserte helsejournal, og truer med å publisere navnet ditt sammen med informasjon om at du har en alvorlig sykdom. Du føler deg hjelpeløs og vet ikke hvordan du skal unngå avsløringen.	A criminal is able to hack your online health journal, which contains information about a serious hereditary disease you have and threatens to publish it with your full name. You feel helpless and don't know how to avoid this disclosure.
A3B1C1	Et annonseselskap plukker opp ditt politiske standpunkt i sosiale medier og sender deg reklame for produkter relatert til partiet ditt. Du bruker hele lønningen på produktene.	An advertisement company picks up on your political stance in social media and they send you advertisements for merchandise related to your party. You spend a lot of money on merchandise.
A3B1C2	Du kjøper produkter fra en nettbutikk for å støtte et politisk parti. Uten å være klar over det, samtykker du til å bli brukt i reklamer. Dette resulterer i at du blir fysisk trakassert av velgere fra et annet parti.	You buy merchandise from an online shop to support a political party. Unbeknownst, you agree to being used in ads, resulting in you being physically harassed by opposing voters.
A3B1C3	Du velger seksuell orientering i en dating app. Basert på denne informasjonen blir du i appen eksponert for reklame om hurtigtest for HIV. Du blir svært urolig.	You select your sexual orientation in a dating app. Based on this information the app exposes you to advertisements of a rapid test for HIV. This causes you a lot of distress.
A3B2C1	Sykepengene du mottar fra NAV blir trukket tilbake som følge av at saksbehandleren din ser på Facebook at du er på ferie utenfor EØS, uten å ha meldt ifra på forhånd.	The sickness benefits you receive from the Norwegian Labour and Welfare Administration (NAV) gets withdrawn as a result of your case worker seeing on Facebook that you are on vacation outside of the EEA, without having reported it in advance.
A3B2C2	Politiets nettpatrulje overvåker din sosiale medier-aktivitet og du blir mistenkt for narkotikahandel, selv om dette ikke stemmer. Under pågripelsen blir du redd og prøver å flykte, men du blir raskt overmannet og skades i sammenstøtet.	A police task force tracking social media activity, finds a picture that puts you under suspicion of drug dealing, although this is not actually true. During the arrest you become frightened and try to flee the scene, but you're quickly overpowered and get injured in the process.
A3B2C3	Du deler utfordringene du erfarer som aleneforelder i sosiale medier. Barnevernet identifiserer deg og begynner å undersøke om du er egnet til å være forelder. Dette stresser deg.	You share the struggles that you are experiencing as a single parent on social media. Child welfare identifies you and starts investigating if you are fit to be a parent. This stresses you.
A3B3C1	På bursdagen din deler en venn en video i sosiale medier der du er full. Sjefen din ser videoen og du mister mulige bonuser fordi du har opptrådt uprofesjonelt. På grunn av tap av inntekt opplever du økonomiske utfordringer.	When your birthday comes around, a friend posts a video on social media of you being drunk. Your boss sees the video and you lose potential bonuses for appearing unprofessional. Due to the loss of income, you experience financial hardship.
A3B3C2	Du endrer sivilstatus på Facebook og tagger kjæresten av samme kjønn. En som er venn med deg på Facebook har sterke meninger om homofili og slår deg ned neste gang de møter deg på gata.	You change your relationship status on Facebook and tag your same-sex partner. One of your Facebook friends have strong opinions about homosexuality, and attack/ assault you the next time they see you in public.
A3B3C3	Familiemedlemmer tagger deg i bilder fra en religiøs begivenhet. Vennene dine unnlater å invitere deg til sosiale sammenkomster og fester på grunn av din religiøse tro.	You are tagged in photos from a religious event by your family members. Your friends avoid inviting you to social gatherings and parties because of your religious beliefs.

Structuple	Norsk item text	English item text
A3B4C1	Du deler dine seksuelle preferanser med en venn i en meldingsapp. En kriminell hacker appen og truer med å dele meldingene med mindre du betaler 10 000 kr. Du betaler.	You share your sexual preferences with a friend in a message app. A criminal is able to hack the app and threatens to share the messages unless you pay 10 000 kroner. You pay.
A3B4C2	Du trykker “skal” på et pride-arrangementet i sosiale medier som alle kan se. En kriminell gruppe peker ut de som er på deltagerlisten og banker dem opp.	You click the "attending" button on a Pride-event on social media, available for everyone to see. A criminal group targets people on the attending list and assaults them.
A3B4C3	Du har deltatt på en sexfest. Et kriminelt nettverk hacker listen over deltakere og truer med å publisere den. De utsetter deg for utpressing, noe som er psykisk belastende.	You attend a sex party. A criminal network hacks the list of participants and threatens to publish it. They expose you to extortion, which is psychologically distressing.