Summer 2023

A Forward-Looking Conceptualization of Information Privacy

David Kallemeyn

Claremont Graduate University

A Forward-Looking Conceptualization of Information Privacy

By

David Kallemeyn

Claremont Graduate University

2023

Approval of the Dissertation Committee

This dissertation has been duly read, reviewed, and critiqued by the Committee listed below, which hereby approves the manuscript of David Kallemeyn as fulfilling the scope and quality requirements for meriting the degree of Doctor of Philosophy in Information Systems & Technology.

Wallace Chipidza, Chair
Claremont Graduate University
Assistant Professor of Information Systems & Technology

Terry Ryan
Claremont Graduate University
Professor of Information Systems & Technology

Chinazunwa Uwaoma
Claremont Graduate University
Research Assistant Professor of Information Systems & Technology

Abstract

A Forward-Looking Conceptualization of Information Privacy

By

David Kallemeyn

Claremont Graduate University

Privacy is a fluid and ever-evolving concept, studied across multiple fields and with numerous definitions. Privacy research in information systems (IS) is extensive yet has not traveled far beyond the IS realm and fully engaged in the broader conversations being had with regards to privacy. This research seeks to define a larger sense of privacy that integrates the many working definitions across fields, along with related concepts, and to develop an alternative framework that can account for the constant technological and socio-technical changes through which to engage in privacy research. One such framework is developed and tested, grounded in the idea of the relative distribution of digital information decision rights across groups within a society, demonstrating the utility for future-oriented research that allows for active theorization that can adapt to rates of technological progress and resulting socio-technical changes.

Keywords: Information Privacy, Privacy Concerns, Anonymity, Surveillance

Acknowledgements

I would like to express my gratitude to all those who helped make this possible. To my committee chair for sage advice, always being available, and willing to discuss anything of interest from the finer elements of research design to the hot-button topics of the day, week, or month – I will remember those discussions fondly. To the members of my committee for their time in reviewing and providing excellent feedback, and willingness to serve on my committee. To all my professors for memorable and enjoyable classes, their patience and wisdom during the lengthy journey. To my classmates for all the lively discussions and ideas that made the journey that much more enjoyable and enriching. To my teacher ed colleagues for their encouragement and for illuminating what a good teacher, mentor, and student is all about, serving as a guidepost as to what to strive for.

I would also like to say a special thank you to my family, for their patience along the way. To my amazing wife for all her support and willingness to shoulder so much of the load throughout my studies, I am forever in your debt. To my children who were (almost) always understanding when dad needed to work, and were able to get a head start on their careers as video game designers as a result.

To Hotrod, for being a good boy.

To all, DBAT.

TABLE OF CONTENTS

Chapter 1: Introduction

The information age has substantially altered notions of and conversations surrounding the notion of privacy. A large body of research both within and outside of IS relating to privacy has been produced, and yet a single definition of privacy remains difficult to pin down, often varying by field or timeframe. The fact that ideas of privacy - both what it is and what it is not - continue to evolve is not a new phenomenon (Smith et al 2011); however, the ubiquity of devices, data collection, transmission and use in today's networked digital world has placed increasing pressures on prior conceptions of privacy and prompted much discussion about its future and role in society. Countries around the globe are grappling with the ubiquity of digital information and its consequences, as evidenced by the number of countries considering or adopting new digital privacy measures. It is becoming increasingly apparent that privacy does not exist in a vacuum, and that it is not a 100% user choice; rather, it is greatly affected by attitudes, policies, and practices of society at large intersecting and interacting with technology, and therefore there is a clear need to better understand how various social structures affect privacy, especially the relative distribution of rights among various groups in society.

The IS field has researched privacy extensively and arrived at well-defined ideas of information privacy concerns primarily grounded in rigorous, empirical work in the positivist tradition (Smith et al 2011). Despite the well-crafted and rigorous work done in IS relating to privacy, IS scholars note that the primary voices in policymaking and strategy forming contexts continue to be computer science, social science, and law; the work of IS scholars regarding privacy is not as prevalent in the public square (Belanger and Xu 2015, Dinev 2014). Without analyzing the underlying forces that influence privacy and addressing the inability to reason about privacy in a forward-looking manner, it is unlikely that merely extending current IS constructs and research streams that primarily focused on individual action and motivations will achieve the desired outcomes of moving into the larger privacy discussion and effectively deal with privacy challenges.

Therefore, the current work has the following goals:

(1) to expand privacy research into more future-relevant modes of theorizing via an embrace of research ideals that include more speculative work and dialog-based theorizing, and

(2) integrate IS privacy ideas with those present in other fields in an effort to unify notions of privacy to an extent that IS research can effectively speak to the privacy conversations taking place in other fields as well as the broader public sphere, to

(3) utilize ideas from 1 and 2 above to develop a new framework through which to approach privacy research that better accounts for social structures, and

(4) utilize the framework to assess the impact of theoretical changes to existing distributions of information decision rights across various countries.

To that end, the current work retraces the tracks of IS research related to privacy and considers future avenues of exploration in more of a discussion-based manner as opposed to single oracle of truth (Burton et al 2021). This includes re-evaluation of prior recommendations made within IS research, as well as on future potential paths of research, thinking about whether we are asking the right questions to grasp and contend with the problems faced. The theoretical work done utilizes inductive reasoning whereby premises can offer a measure of support for conclusions, which is appropriate in cases with extensive existing literature with many competing interpretations and/or conceptualizations (Leidner and Tona 2021). Additional theoretical foundations include recent departures from inherently backward-looking empirical studies in an embrace of observational frames that are not inhibited by what was, but can provide insight as to what may be imagining possible lived futures (Hovorka and Peter 2021). Finally, the work utilizes a newly proposed framework for engaging in privacy research via a survey of international students and reports on the findings.

Chapter 2: Foundational Research

Privacy

In the western world, notions of privacy can be traced back to the middle ages, where it existed primarily in the form of laws that ranged from restricting certain actions such as trespassing and eavesdropping to a 1324 English law mandating the interception and inspection of all incoming mail in defense of the King (Marshall and Thomas 2017). The crystallization of the idea of privacy as an individual right was articulated by Samuel Warren and Louis Brandeis in 1890 as the "general right of the individual to be let alone" (Warren and Brandeis 1890, p. 205). US supreme court justice William Douglas expanded the notion of privacy to include personal choice in 1967: "Privacy involves the choice of the individual to disclose or to reveal what he believes, what he thinks, what he possesses..." (Douglas 1967, as cited in Zuboff 2015, p. 83). Other works better detail the full evolution and application of privacy across fields and time periods, including its use in law, philosophy, psychology, economics, and of course the social sciences and IS (Dinev et al 2013, Smith et al 2011); however, from its initial entry into the public square privacy has maintained a core that relates to an individual's decision and/or choice.

Shift from the physical to the informational

While there will always remain two key categories of privacy, the physical and the informational, the relative prominence of each has undergone a shift to the point that the most frequently discussed (and researched) form of privacy is now the informational, not the physical (as it had been for much of privacy's history). The key driver in the predominance of information privacy has been the digitization of information. As discussed in Belanger and Crossler's review of IS information privacy research, Roger Clarke outlined four dimensions of privacy: privacy of a person, personal behavior privacy, personal communication privacy, and personal data privacy (Clarke 1999, as cited in Belanger and Crossler 2011). Revisiting these dimensions now, communications are predominantly digital, and, combined with the interconnectedness of modern devices and systems, 'personal communication privacy' and 'personal data privacy' overlap to such an extent that they can be merged. Following a similar rationale, 'personal behavior privacy' has largely been subsumed here as well, at least for individuals using mobile devices (location data, check-ins, edge device monitoring, facial recognition, etc.) and/or social networks (sharing of behaviors). That leaves what is referred to here as "digital privacy" for Clarke's latter three dimensions, along with "privacy of a person". For individuals utilizing digital devices and, increasingly, those that do not (due to the use of inferential methods and surveillance), "privacy of a person" is encircled by this "digital privacy", and the two become largely indistinguishable. Thus, the broader term 'privacy' is useful here, and is adopted to discuss the encompassing idea of privacy in the information age. Prior research has also equated privacy and information privacy, especially given that physical privacy comprises an ever-shrinking aspect of privacy due to the expansive generation and collection of digital information (Dinev 2014).

Therefore, the term 'privacy' is adopted here in lieu of information privacy, although specific mentions of research specific constructs may still use information privacy or other terms. The fallback to the use of privacy is also helpful in drawing the connection from the origination of the term to the current discussion, as many of the same observations about the nature of privacy are still relevant today. Another benefit in unifying the discourse at a broader scale is that it also enables a common lens through which to synthesize the multitude of ideas surrounding privacy.

What is Privacy?

Belanger and Crossler define privacy (information privacy) as "the desire of individuals to control or have some influence over data about themselves" (Belanger and Crossler 2011, p. 1017). Most if not all definitions encountered in the literature include some aspect of control, emphasizing an individual's agency. In researching 'surveillance capitalism', Shoshana Zuboff furthers that notion of agency in positing that the exercise of privacy involves choice (the choice to either share or keep secret), and therefore any type of right to privacy necessarily confers decision rights (Zuboff 2015, p. 83). It is these concepts about individual choice and agency/decision-making concerning information about oneself and potential future uses that is considered to embody the notion of privacy for purposes of this discussion. Note that this conception of privacy is inherently forward-looking, seeking to preserve both current and future decision-making. When combined with Margulis' conception of privacy, the following definition is arrived at for use:

> *'control over information that regulates access to the self in order to enhance current and future decisional and behavioral choice' (Margulis 2003, p. 415)*

Tracking the evolution of ideas around privacy and its investigation across fields, two key observations regarding privacy emerge: (1) privacy appears to be an ever-evolving concept that varies across time, field, and arguably individual, and (2) as a result of the first observation privacy will continue to change and be affected by new modes and frontiers of information accumulation. It is the second observation that is the most crucial to the future of IS research regarding privacy and for society at large, as the ability to presently theorize and reason about potential privacy futures is essential to its ability to be exercised in the future.

The pace of digitization and information collection and use has continued to grow, and has given rise to new avenues of concern. Consider the following quote from the sociologist James Rule:

> *Any member of a modern, highly 'developed' society is apt to feel that he inhabits two worlds at once. One is the ordinary social world or events, people, relationships and so on as they impinge directly on experience. The other is a 'paper world' of formal documentation which serves to verify, sanction and generally substantiate the former experiential reality.* Rule 1974, p. 13).

This comment referencing the creation of an alternate world or 'identity' as a result of paper recordkeeping, and the idea that there are but two instances of an individual seem trivial compared to the scale of data collection in the information age; the 'real' and the 'paper' are dwarfed by digitization and networking. Between user-generated sharing and digital participation and the collection, reselling and shuffling of data via the data economy, there is virtually no limit to the number of 'existences' an individual can inhabit. Each platform has its own 'you', data sellers and resellers continually repackage and create "you's" in perpetuity. It is hardly surprising then that individuals may increasingly encounter situations of concern surrounding their privacy.

IS research on Information Privacy Concerns

The result of the multitude of technological advances in the information age and the concerns it has spawned has led to the topic of privacy being a heavily researched area in IS. IS has primarily operationalized privacy research via the construct 'Information Privacy Concerns', or individuals' perceptions regarding privacy, but more recent discussions within this thread of IS research has emphasized the need to explore additional avenues and move beyond IPC as the sole measure of privacy. Information privacy concerns have traditionally been measured by one of two instruments - Smith's CFIP instrument (Smith et al 1996) or the IUIPC (Malhotra et al 2004).

In 2011, MISQ published a special article focused on privacy research in IS which included a number of comprehensive works that encapsulated the state of privacy research in the field and crystallized some key ideas that would drive future work.

The most discussed constructs in IS privacy research according to Belanger & Crossler in 2011 were information privacy concerns, e-business impacts of information privacy, and information privacy attitudes and practices. Secondary topics included trust, culture, security, the economics of information privacy, surveillance, personalization, risk, marketing, and control. They further identified a third tier of topics that was largely present in conference proceedings but largely absent in journals: tools and technologies designed around information privacy. Primary outcomes studied were related to intention to use, interact, or disclose information (Belanger and Crossler 2011).

Smith et al conducted an interdisciplinary review of privacy-related research, synthesizing existing work into the APCO framework, which describes the relationship between privacy antecedents, information privacy concerns, and outcomes (such as decision to use, regulation, etc.). This refined the conceptualization of information privacy and enabled the analysis of the relationship between information privacy and related constructs while noting the contextual nature of the relationships. Of particular importance are the identified antecedents of privacy concerns: privacy experiences, privacy awareness, personality differences, demographic differences, and culture/climate.

Pavlou added economic perspectives to the discussion of information privacy research, represented by concepts such as information asymmetry, and concluded that there is little IS research can do to further define information privacy and information privacy concerns (Pavlou 2011).

The primary reason for dedicating space to some of the key ideas in the 2011 work here is to allow for an analysis and contextualization of identified works from 2012 to now in terms of the recommendations made in 2011; in other words, which suggestions were heeded, and which areas remain open questions. The 2011 recommendations used to guide the discussion are: integrate new (related) ideas, expanded treatment of information privacy concern antecedents, expanded treatment of outcomes, and conduct research across the identified levels of privacy (individual, group, organizational, societal).

Post-2011 Privacy Research

New Related Ideas used

Recent IS privacy research has continued to expand the application of ideas from other fields as well as novel methods of exploration as well. The fields that appear to hold the most relevance for are behavioral economics and psychology, with privacy research incorporating a host of cognitive factors and biases (Dinev et al 2015, Acquisti et al 2015, Adjerid et al 2018, Kehr et al 2015). Recent work has even expanded beyond individual psychological approaches to include social psychology and group behavior (Belanger and James 2020). Economics-related work has expanded from privacy calculus related analysis to attempts to estimate the value of data to individuals (Spiekermann and Korunovska 2017), and scholars have traced the anthropological origins of privacy to demonstrate that privacy is a socially-developed concept as opposed to an innate part of human consciousness (Dinev 2014). It is clear that a broad knowledge base is brought to bear in examining information privacy. In addition to the inclusion of a broader array of fields, IS privacy research has also examined new constructs, including privacy uncertainty which examines the difficulty users face in assessing privacy (Al-Natour et al 2020). Research methods have also been used in novel ways, with privacy researchers employing qualitative cross-cultural comparisons (Miltgen and Peyrat-Guillard 2014) as well as design science research methods to guide privacy impact assessments which can speak to the broader conversations taking place surrounding privacy by design efforts (Oetzel and Spiekermann 2014). Other works have broadened IS privacy conceptually, looking at conceptions of identity in relation to information systems (Bansal et al 2015, Whitley et al 2014) as well as frameworks for researching the darknet (Benjamin et al 2019), which is poised to grow in relevance as IS research branches out into other privacy related topics.

Treatment of Antecedents

Researchers have looked at new salient factors impacting existing antecedents as well as studied additional antecedents to information privacy concerns. An enhanced APCO model added level of effort as well as peripheral cues, biases and heuristics as factors that impact the privacy calculus (Dinev et al 2015), and additional studies have examined perceived control and perceived risk as determinants of perceived information privacy (Dinev et al 2013). IS researchers have also explored how the relationships between the constructs of privacy experiences, privacy awareness, trust, risk and benefits impact individuals' disclosure behaviors, finding that privacy experiences and privacy awareness are significant predictors of privacy concerns (Ozdemir et al 2017).

Treatment of Outcomes

While intentions as an outcome variable are still widely used in IS privacy research, research has examined behavioral outcomes in terms of how they are impacted by external stimuli (Dinev et al 2015) as well as specific outcomes such as sharing/disclosure behaviors and privacy protective behaviors (Belanger and Crossler 2019). Despite its appearance as an outcome in the APCO framework and its prevalence in current public discourse, regulation has received little treatment in the IS literature (Dinev 2014).

Treatment of the multilevel nature of information privacy

The overwhelming majority of IS research remains at the individual level, with occasional work covering societal privacy-related issues (Riemer et al 2020). Even rarer still is the work that examines privacy at the group level, although work has been done to establish conceptual models that allow researchers to reason about both individual information privacy as well as co-owned information (Belanger and James 2020).

The IS community has demonstrated a willingness to engage in self-reflection, and is clearly interested in expanding beyond existing literature; in the case of privacy, researchers have made increasing calls to move beyond traditional, well-established IS information privacy constructs such as information privacy concerns, and to integrate work done in other fields (Dinev 2014, Belanger 2015). However, much work remains to be done here to guide IS privacy research in new directions; the bulk of IS research surrounding privacy still focuses on the individual level, is predominantly concerned with intentions to disclose or privacy concerns, and has not greatly expanded work on outcomes. Belanger and Xu in 2015 revisited the 2011 assessment of the state of privacy research in IS, and concluded that not a lot had changed (Belanger and Xu 2015, Belanger and Crossler 2011).

Moving from information privacy to privacy

Stepping back from information privacy concerns and specific constructs that appear in the IS literature, it is instructive to take a look at the different types of privacy in order to reason about how to arrive at a more unified conceptualization of privacy. Smith et al note there are two broad categories of privacy in the literature: value-based and cognate-based. Value-based ideas of privacy include the idea of privacy as a right most often associated with law or ethics as well as the notion of privacy as an economic good that possesses value (positive or negative). Cognate-based interpretations view privacy as either a state, primarily envisioned along a continuum, or as an expression of control (Smith et al 2011).

Privacy as an economic good (privacy calculus, cost/benefit vs. risk)

Privacy as a state that contains varying degrees of limited access places emphasis on individual choice (Leidner and Tona 2021), having its origins in economic arguments surrounding information (and privacy) as an economic good used in either the "production of income or some other broad measure of utility or welfare (Posner 1978, p. 19). Such economic and rational choice approaches frequently analyze the costs (loss of privacy) and benefits (personalization, obtain services and/or goods, etc.) of sharing information, however the critical premise here is that individuals do in fact have a choice (and the agency to make said choice). In many situations, individuals do not have a real choice as the tradeoffs and reciprocities proffered are not the product of genuine consent (Zuboff 2015). A prime example are website cookie agreements - websites are required to get your 'permission' to store persistent data on your device prior to your accessing the site, however your only choice is to allow the behavior or be denied access entirely; for a critical service such as medical advice or procurement of medical services, there is no true choice. As Zuboff correctly acknowledges, trusted professionals like doctors and lawyers are held accountable by professional licensing, sanction, and public law - there exists a framework of reciprocities and mutual dependencies that promote positive outcomes for all parties (Zuboff 2015). Cyberspace has no such framework, no mutual dependencies to ensure that users are in the end made better off. In the privacy realm, these types of economic frameworks need to question the degree to which a true choice in fact exists in trying to reason about why individuals act the way they do.

Privacy as a state

The implicit question here is: do individuals possess the agency to arrive at the desired state? Not with respect to a single decision to share or disclose, but can individuals effectively exert decision rights over their information across a meaningful portion of their existence? The state-based conceptions of privacy, while useful, need to contend with the reality that the enaction of privacy as a state is not wholly at the discretion of the individual. Clearly, in cases that concern self-disclosure (such as a social media post) an individual has the agency to act or not act, but there are situations where this is not the case. In cases that are inferential, where the individual has not provided information that is discernable by automated systems (facial recognition software, for example), the individual has no means of arriving at the desired state. Strictly cognate-based approaches can yield fruitful micro-results in the right contexts, however even when applicable they are largely unable to account for future behaviors as they are silent on surrounding factors that can heavily sway actions and perceptions in the privacy arena. Much research on privacy and behaviors, not as much on the surrounding environs and incentives in place.

Privacy as a right

Privacy as a right originated in the legal field, and yet the government has stopped attempting to define exactly what privacy is due to the difficulty of the task. This conception of privacy is one that many IS researchers dismiss due to its reliance on normative arguments and its inherently subjective nature. While the specifics of privacy are impossible to define and attempting to imagine a list of every action that could possibly embody or impinge upon the term is fruitless, it is important that IS researchers acknowledge that privacy rights are at their core decision rights, and they exist whether they are explicitly acknowledged or not. To see why this is the case, consider geo-location and the ability to track individuals' whereabouts. The fact that there were no protective mechanisms in place for individuals when this technology was introduced does not imply that individuals should not ever have any choice in whether or not their phone carrier or Google or any other of a host of companies can perpetually track their whereabouts, it simply means that those rights were implicitly assigned elsewhere. The collection of this data conferred rights to the collector, whether intentional or not - rights such as who to share it with, how it is used, etc. Privacy as an individual right is not the right to maximize an individual's privacy at every possible opportunity; privacy as a right simply acknowledges that the collection and storage of information confers rights that can have an impact on the choices available to an individual, and these rights and their impacts on choices should be made visible and discussed. Consider the following: "Although technology is a morally neutral object (Kass 2002), the impact of technology on human life is not morally neutral and neither are those designing, using, and benefitting from such technology use" (Leidner and Tona 2021, p. 364-365).

This quote perfectly illustrates the centrality of values and the societal in examining the technological; how choices and future behaviors of individuals are constantly shaped even in the absence of any explicit decision to do so. Discussions surrounding privacy as a right and as a value are therefore critical to fully understanding privacy and its place in IS research, and the CARE theory (claims, affronts, response, equilibrium) illuminates a potential path forward in terms of theoretically integrating technology with values and ethics and elaborates a new approach to data digitalization and evaluation of its consequences (Leidner and Tona 2021).

Privacy as ever-evolving

As a social construct, the boundaries surrounding notions of privacy will always change. In today's information age, these boundaries are driven primarily by technology, and speculating as to the next privacy frontiers is an invaluable tool for researchers in navigating uncertain futures. As discussed earlier, the convergence of all forms of information into the digital means that once a new frontier is mapped to data and interpretable, it becomes an additional source that can not only be verified but also uncovered and manipulated, often with unintended consequences (see Zuboff's discussion of "informating", Zuboff 2015).

Systems to detect and collect information about innate properties or states of things are being developed and deployed, such as information about an individual's genetic makeup or emotional state. In the case of emotional state, facial recognition technology is being deployed to track both the behavioral and emotional state of students, allowing schools (and technology platforms) to extract more information about a person than they choose to reveal, or in some cases are even consciously aware of (Crawford 2021). This type of data collection implicitly grants decision rights over emotional state and behavior to those deploying the technology, and we are approaching the point where these means of data collection can arrive at information the individual remains unaware of. A similar potential exists for accumulation of data and implicit assignment of rights across a host of frontier technologies: Internet-of-Things, robotics, genetics, biometrics, nano-treatments and devices, persuasive technology, virtual & augmented reality, inferential methods, and a host of as yet unidentified future developments (for an ethical treatment of many of these topics, see Royakkers et al 2018); as these new developments expand the reach of digitization, nothing in the past will have prepared individuals nor will defensive barriers have been established unless research can contribute in forward-looking ways. An interdisciplinary approach is needed to deal with issues that clearly span multiple fields (technology, biology, and society in the case of biometrics), and this is happening in the policy realm in the case of biometrics via bodies such as The Citizens' Biometrics Council.

With IS existing at the intersection of the technological and the social, it is uniquely positioned to contribute influential research in these areas, especially in the realm of privacy. The ability of privacy frameworks to be able to reason about the future will be of increasing importance as impacts on non-users of technologies as well as impacts on users beyond what they are aware of become commonplace. It is important to have a conception of privacy broad enough to encompass expansions into new frontiers, and this expansive interpretation of privacy have been around since Warren & Brandeis' writings, where the fact that an action or even appearance of an individual may be ephemeral, but should be no less protected than something that is recorded or written:

> *For the protection afforded is not confined by the authorities to those cases where any particular medium or form of expression has been adopted, nor to products of the intellect. The same protection is afforded to emotions and sensations expressed in a musical composition or*

> *other work of art as to a literary composition; and words spoken, a pantomime acted, a sonata performed, is no less entitled to protection than if each had been reduced to writing. The circumstance that a thought or emotion has been recorded in a permanent form renders its identification easier, and hence may be important from the point of view of evidence, but it has no significance as a matter of substantive right. If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression.* (Warren and Brandeis 1890, p.206)

Moving IS work on privacy into the popular discussion: Integration of Privacy, anonymity, surveillance, etc.

A number of IS researchers have expressed concern at the lack of IS researchers' voices in discussions surrounding privacy. In an attempt to ease this transition, it is fruitful to assess privacy-adjacent topics in existing literature as well as those shaping discourse beyond IS, and look for opportunities to integrate them. This section seeks to tie together IS strands of research, historical concepts of privacy, and ideas related to Zuboff's 'surveillance capitalism' - including its structure and incentives - into the privacy research discussion.

IS researchers have noted the difficulty in differentiating the myriad of privacy-adjacent concepts and constructs, as they often contain overlapping ideas (Margulis 2003, Smith et al 2011). Concepts explicitly called out as distinct from privacy include security, secrecy, and confidentiality (Smith et al 2011). Further, a number of these terms have been identified as identity management tactics - anonymity, secrecy, confidentiality, and transparency (Zwick and Dholakia 2004). Three of these tactics - anonymity, secrecy, and confidentiality - are also conceptualized as determinants of information control (Dinev et al 2013). In addition to the efforts at differentiating what is and isn't privacy, IS research has increasingly attempted to integrate historical treatment of privacy from other research traditions; one such effort and places a number of privacy correlates in an expanded APCO framework (Dinev et al 2015).

In an effort to determine which topics are more heavily covered in core IS research, a number of keyword searches were done using Web of Science database.

From readings, an initial list was assembled that embodied other avenues of exploration and topics seemingly related to privacy. The primary search term was, of course, privacy. Other initial search terms identified were (the * denotes a wildcard, allowing the search to be done for the desired stem) anonym*, decentraliz*, centraliz*, distributed, security, secrecy, and confidentia*.

Table 2.1 shows the keywords with more significant numbers of hits over the time period from 2000 to present, within the SSB8.

Table 2.1. Web of Science research results, SSB8, 2000 - 2021

Keyword	*MISQ*	*Other B of 8*	*Total B of 8*	*MISQ, 2012+*	*Other B of 8, 2012+*	*MISQ, % 2012+*	*Other B of 8, % 2012+*
Privacy	31	126	157	20	88	65%	70%
Anonym*	10	17	27	7	12	70%	71%
Decentraliz*	9	18	27	7	8	78%	44%
Centraliz*	7	19	26	4	7	57%	37%
Distributed	32	107	139	16	38	50%	36%
Security	59	161	220	38	100	64%	62%
Secrecy	0	4	4	0	2	NA	50%
Confidentia*	1	10	11	1	5	100%	50%

2012 was used as a key comparison metric due to the impact of the 2011 MISQ special issue on privacy in attempt to measure popularity of the topic over time. From Table 1 it is apparent that security is the most-published topic in the SSB8, followed by privacy. While the share of 2012 and later articles in MISQ is roughly constant for both privacy and security, in the remainder of the SSB8 publications privacy articles are more recent (70% of articles since 2000 published 2012 or later, compared to 62% for security).

In reading through the abstracts, the term distributed was primarily used in non-privacy related contexts, such as software development teams and other management-related work, and therefore no additional analysis of these articles was done.

The next round of terms were drawn from a combination of other terms of interest that often overlap with ideas of privacy as well as the tags for articles that appeared in the 157 results for 'privacy' shown above. Other related terms were: censorship, darknet, and co-option. The tags appearing in the privacy results were: surveillance, and data economy. Results of the second wave of terms is shown in Table 2.2:

Table 2.2. Web of Science search results: additional terms (SSB8, 2000 – 2021)

Keyword	*MISQ*	*Other B of 8*	*Total B of 8*	*MISQ, 2012+*	*Other B of 8, 2012+*
surveillance	1	27	28	DNS	22
Censor*	0	6	6	DNS	4
Co-opt*	1	1	2	DNS	1
Darknet or ‘dark web’	1	0	1	DNS	0
Data economy	9	NA	NA	NA	NA
“Data economy”	0	DNS	DNS	DNS	DNS

DNS = did not search

Surveillance had the most matches here, primarily in non-MISQ SSB8 papers. 'Data economy' was used initially as separate terms, which returned 9 MISQ articles but none were actually related to the data economy as an entity, they simply addressed data and some sense of the word economy. No further journals were searched for data economy, and the combination of the terms in succession returned no results in MISQ and was also abandoned in future searches. There were also very limited results for either darknet or the 'dark web'. Although these terms may be useful in other contexts, they do not appear to be salient features of SSB8 scholarship at this time.

In an effort to determine the potential relevance outside IS research, the keywords darknet or 'dark web' were used in Web of Science across all journals from 2000 to present, resulting in 153 matches. This group of publications was characterized by limited numbers of citations (results 52-153 were cited fewer than five times each) and were largely non-IS related publications. There does not appear to be much connection to the streams of privacy research in IS and there works, yet there is certainly a thematic connection between anonymity, privacy, and the dark web. Much of this work is done at the implementation level regarding specific technologies and is not typically concerned with the constructs related to privacy. However, the discussion between the two can be valuable moving forward. This is the primary reason they are included in this analysis despite not being directly comparable to existing IS research related to information privacy and operating at different theoretical levels.

Privacy-related concepts and work in other fields

Work in other fields

Many fields research privacy and privacy related concepts, and there are endless articles regarding the potential risks of new technologies and their implications for privacy. Ethical discussions center around privacy, autonomy, security, human dignity, justice, and balance of power (Royakkers et al 2018, Leidner and Tona 2021). Economics work related to privacy includes concepts such as information asymmetry, incentives, and cost-benefit analyses (Pavlou et al 2007). Behavioral economics, at the intersection of economics and psychology, has much to say about individual behavior (far too much to list here).

As a result of the number of fields investigating privacy, the number of concepts that have been associated with privacy is vast. The search terms outlined above are a mere sampling of such topics and is not exhaustive. It is beyond the scope of this paper to examine each of these related terms and where they would fit conceptually in relation to privacy (and each other) as there are simply too many, but the current work is an effort to arrive at a conceptualization of privacy that allows them all to be situated and discussed in their own right. To that end, some of the individual ideas are discussed below.

Privacy-related concepts

Anonymity. The relationship between privacy and anonymity is often misunderstood; clearly anonymity and privacy are related, but they are also distinct and often at odds with each other in implementation. Privacy combines the ability to identify actors with an inability to have knowledge of their actions or behaviors; conversely, anonymity combines knowledge of actions or behaviors with an inability to identify actors. In each case, there is knowledge of either identity or actions, but not both. Technological implementations are often faced with a design parameter trade-off in terms of privacy and anonymity. Additionally, anonymity is trustless while privacy necessitates trust. In relation to the privacy research discussed here, this is a key point, as surveillance capitalism seeks to replace the need for trust with certainty of being able to monitor conditions of a contract by observing the previously unobservable. Thus, a strictly computer-mediated world strips away governance and the rule of law as it has no need for trust, authority, and ultimately choice. According to Zuboff, authority is derived from social construction animated by shared foundational values, and when authority is replaced by technique there is no longer room for dialog or reciprocity (Zuboff 2015); Hannah Arendt asserts that human fallibility in the execution of contracts is the price of freedom (Arendt and Canovan 1998). It is this element of choice that privacy is concerned with, the ability to have decision rights over behaviors and actions.

Secrecy. Zuboff argues that privacy and secrecy are sequential, that secrecy is an effect of privacy (Zuboff 2015). In the IS tradition, secrecy is an identity management tactic, an exercise of control (Zwick and Dholakia 2004, Dinev et al 2015); however, this interpretation confuses where the choice lies - if privacy involves a (socially negotiated) choice, then the ability to engage in secrecy depends on this choice. Conversely, secrecy does not appear concerned with choice or decision rights in its definition.

Data Economy. There is no way to discuss digital privacy without discussing the data economy. The separation of individuals from data about their interactions and behaviors is at the core of ideas of choice and decision that embody privacy. Discussions surrounding privacy are driven in large part by the demand for data, the expansion of data, and the overall accumulation of information rights as a result of digitization. Zuboff notes that this "logic of accumulation produces its own social relations and with that its conceptions and uses of authority and power" (Zuboff 2015, p.77). It seems important, then, that IS privacy research expand to include the context of the larger data economy and the associated incentives for accumulation of information regarding individuals.

Surveillance. Surveillance is a tactic that can be employed by any agent, including an individual, a corporation, government, or other entity. If privacy allows a decision as to where on the secrecy-transparency spectrum an entity wants to be, surveillance is a way to redistribute privacy rights and circumvent that decision, resulting in a loss of choice on behalf of the surveilled.

Security. Security is an expansive term, and a treatment of that term is beyond the scope of this work. However, some commentary regarding technological solutions to secure privacy seems warranted. There are a number of technologies marketed as privacy enhancing, and they often fall into one of two philosophical camps: technologies that seek to limit the information that can be gleaned from their use, and those that seek privacy by virtue of limiting who has access to the data (e.g., enhanced authentication measures). The vexing problem of privacy via security is that the main solution proposed is also the main driver of its abuse. The ever-evolving security solutions geared towards identification and authentication - thumbprints, retina scans, DNA, etc. - open new avenues of information flows subject to accumulation, which reduces the overall future space within which individuals can operate. Additionally, purely technical solutions operate using the same infrastructure via which individuals are surveilled, and it is unclear as to whether these two functions (privacy and surveillance) can remain siloed from each other operating over the same physical infrastructure.

Chapter 3: Theoretical Foundation for Forward-Looking Privacy Frameworks

Existing Foundational Frameworks

In reviewing the IS literature regarding privacy, there are a number of challenges: integrating work done in other fields, addressing specific identified areas for future research, and entire areas of research that have to this point been largely ignored. Some of the most pressing questions repeated over time in IS' own assessment of its work include: the need to account for cultural factors and values, the need for more research on privacy as a multilevel concept, specifically at the group level, and moving beyond information privacy concerns to actual behaviors and outcomes.

Most IS research regarding privacy remains solely positivist, user-centered modeling (Smith et al 2011, Belanger and Crossler 2011, Belanger and Xu 2015). IS researchers have heeded the call to account for additional contextual factors as evidenced by the enhanced APCO model that includes cognitive biases and external cues (among other factors), as well as expanded models that include examination of privacy correlates such as regulatory expectations (government), determinants of perceived risk and benefits of info disclosure (individual privacy calculus), information sensitivity (contextual differences), and the importance of information transparency (organizational influences) (Dinev et al 2015, Dinev et al 2013). Current models may no longer assume rational actors, but they are still framed in ways that provide agency and frame of reference only to the individual user of a particular technology at a particular moment in time - reliant on perceptions of trust, privacy concerns (beliefs, attitudes, perceptions), risks/costs, and benefits. To see how this may be an incomplete picture, consider the question of who determines the amount of cognitive effort required to perform a task such as changing a privacy setting. Traditional IS frameworks may consider cognitive load, compare different user responses across different platforms, or examine the perceived benefit of such actions; while such analysis is beneficial, there seems to be a hidden question that is left unasked: in what ways is the platform determining user responses through its design? So-called 'dark patterns' (or anti-patterns), where known desirable user actions are disincentivized or made exceedingly difficult by the platform developer, are fairly common, and are directly related to the steering of decision and choice on the part of users. Therefore, the incentive structures in place, goals of apps and/or platforms have a largely unacknowledged role here. Consider another question: who is 'responsible' for the preservation of one's privacy? In many IS models, it is implicit that the individual is responsible, overwhelmed though they may be, for their use choices and privacy decisions. Yet the answer to the question depends on the assignment - or lack thereof - of rights. It is apparent, then, that privacy research needs to extend beyond the individual actor (and associated idiosyncrasies of the human brain) into the underlying incentives and construction of society. If corporations (and platforms) are able to monitor and potentially modify behaviors, frameworks need a way to reason about these possibly subtle but influential factors. The presupposition for the relevance of individual-centric models in IS research is that humans have a way of reasoning about the systems they participate in (feedback loops or basic understandings of how they operate), and at present these systems are almost entirely opaque and becoming increasingly so (Zuboff 2015).

The economics stream of privacy research has much to contribute to a type of framework where incentives interact with the distribution of rights and information asymmetries are prevalent (Pavlou et al 2007, Akerlof 1970). In the current environment in the US, incentives prioritize the pre-emptive taking and claiming of rights in the absence of forward-looking protective measures (Zuboff 2015). However, the economic incentives analyzed in IS privacy research are potentially the wrong ones - further analyzing individual incentives surrounding decisions to share individual pieces of information feels like a dead end, as the conversation at large turns to an examination of the societal, regulatory, and financial incentives that impact people's lives. Governments in Europe and elsewhere are beginning to engage in efforts aimed at re-distributing some of the information and data rights that have been accumulated by global technology firms, and it appears that this will likely increase.

Re-imagining IS frameworks

If the goal is to increase the reach of IS privacy research and include this stream of research in the public discussion square, then it needs to be reorganized and re-purposed to better fit this ambitious goal. The philosophical and psychological definitions of privacy that revolve around a 'state of limited access or isolation' no longer encapsulate the entire picture; in an artificial intelligence/machine learning and (digital) surveillance society, individuals rarely have the choice to isolate, and one's 'isolation' (digitally speaking) says as much and in some cases more about someone than their participation.

Recent work in IS has risen to the task of examining broad, grand theories (Leidner and Tona 2021) and imagining possible futures via speculation (Hovorka and Peter 2021), illuminating potential paths forward for privacy research. In order to steer society towards a different future where individuals are given choice and agency in terms of how they are treated by technology, researchers need to imagine potential futures and develop frameworks that are forward looking as opposed to strictly backward looking, empirical studies that are frequently unable to keep pace with actual socio-technical changes loosed by technologies (Hovorka and Peter 2021).

The APCO framework has provided a good deal of insight into personal decision behaviors and privacy concerns, but it is perhaps time to take it in a new direction, to disassemble and rearrange while pruning, ultimately integrating with threads of normative and values-based privacy research.

One of the most acknowledged tenets of IS privacy research is the idea of privacy as a multilevel construct - individual, group, organizational, and societal (Smith et al 2011). Clearly privacy manifests itself across multiple levels, but what if the dearth of group-level analysis, rather than suggesting a future path of research, suggests that it is not of primary importance with respect to privacy? What if the levels were adapted to a new framework, each treated as having agency and affecting privacy within a single conceptualization? If each of the levels was translated into a prototypical instantiation, it would allow for all levels to be analyzed within a single framework. The individual level would remain individual, situated within a societal construct, government would replace the 'group' level, and 'organization' would be represented by corporations (and platforms).

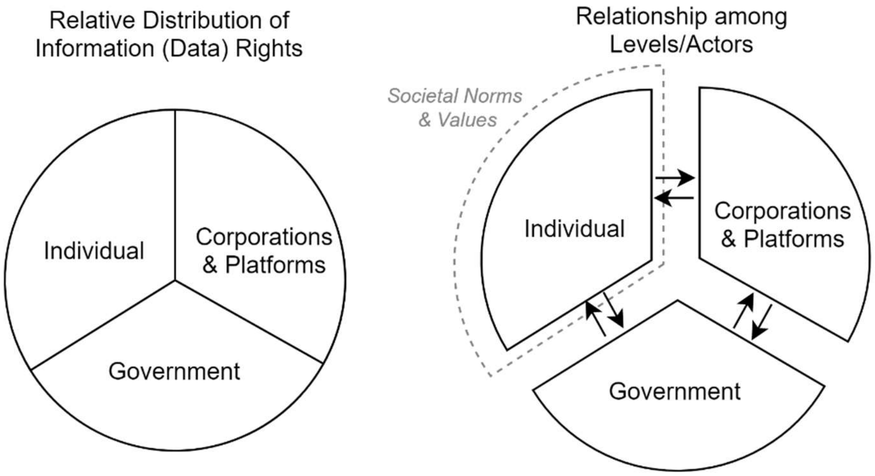

Figure 3.1. Top level conceptualization of information decision rights

Establishing a framework consisting of individuals, government, and corporations would situate the key players in the privacy arena in relation to each other and would open new research pathways. It would answer the calls in IS to undertake research across all levels of privacy as each would be seen as having agency and shaping the digital futures, and would allow analysis of the interplay between them, including the relative distribution of (information) rights and the determinants of and effects of such rights. Government, corporations, and societal norms and values heavily impact technologies and their role in society, especially surrounding values-based ideas such as privacy. This is not intended to foreclose future group privacy research, however it could perhaps be explored in a different conceptual light and left for those researchers to elucidate the relevance/importance/centrality of such work in the privacy domain.

Such a framework would allow for a clearer analysis of the nature of threats to privacy, which would enhance understanding given that privacy either depends on or derives from the nature of its threats (Regan 1995 and Sheehan 2002, as cited in Smith et al 2011, p. 1002). Individuals do not come to concern over privacy in a vacuum, but rather as a reaction to circumstances, and researchers need to be able to reason about these threats in order to truly understand privacy; the key to contextualizing behavior is being aware of the rights and threats to those rights. Threats can come from any of the levels, and the actions of each will have an impact on the others. This will enable richer observations about the role of culture, values, and societal norms as they relate to privacy - an individual's situation in an environment (surrounding corporations, technologies, regulatory environment, nature of government, societal dispositions and values, etc.) is not simply an antecedent of privacy concerns, but a key defining characteristic that would be expected to have a major impact on behavior within a society. This is especially critical given the expansion of the informational frontier that individuals would like to exert choice over in order to preserve their privacy. It would allow for questions similar to the following: where the primary threat model to individuals is government, how does that alter notions of privacy - is it more normative and value-laden? Where the primary threats to an individual are corporate based, is the notion of privacy more economic/transactional?

The suggested conceptualization among actors (previously levels) as manifestations of their most recognizable forms and the interplay between them also enables analysis of changes over time - individuals may change their own desires over time in response to changing conditions, and governments and corporations can similarly exhibit shifts over time. Each of the actors can affect another - governments can surveil individuals, individuals can surveil government actions (often journalists), corporations can surveil individuals, and potentially governments. This allows other ideas connected to privacy to be investigated that were previously challenging to bring together. Actions, instantiations, and constructs can be evaluated in terms of impact within any single actor (level) or impact on the equilibrium (or disequilibrium) that exists among them (macro). Here Leidner and Tona's ideas of equilibrium and disequilibrium surrounding digital dignity are especially relevant as they can be used for each of the primary actors - individuals (situated within society), corporations (organizations), and government.

Even further down a level, it would allow speculation regarding individual artifacts and how it might shift the potential macro-distribution of rights and/or the responses of any individual actor (government, corporation, individual). This would be in accordance with the IS community's desire for additional design science research specifically in the privacy arena (Belanger and Crossler 2011). It would assist the IS community in defining user-beneficial design science that considers multiple stakeholders with an eye towards the accumulation of impacts (equilibrium among actors). Taking a step back and contextualizing each artifact in light of some of the larger forces at play would allow such questions as 'Are there more effective approaches to increasing personal health than additional nudges?' and 'What happens at a societal level when each artifact attempts to optimize individual behavior via nudges?' Due to asymmetries of resources, knowledge, and power, individuals cannot cross the divide and reasonably ascertain the impact of a complex technological artifact or the implicit propositions it offers; there is a distinct lack of feedback loops in place for users of networked technologies inhibiting user-based design science, and it is important that IS researchers investigate these questions.

The future of privacy and IT are inseparable, and the impacts of digitization will continue to reverberate throughout society. The pattern of technology -> concerns -> awareness -> adaptations will continue, and privacy research needs to be forward-looking to have any hope of finding a socially acceptable balance. Different approaches and technologies will be viewed different across cultures, and research would benefit from a framework that considers the actor (individual, corporation, government), the relevant threat vector(s), and potential sources of resolution (who has agency to implement). Ideas of equilibrium and interactions identified here find much in common with efforts surrounding the impacts of digitization of information, specifically the equilibrium/disequilibrium approach to data dignity (Leidner and Tona 2021).

IS privacy researchers have the difficult task of grappling with the ever-changing boundaries of privacy as well as the need to practically evaluate specific technologies and impacts on privacy. To rise to this task will require an ability to conceptualize an ever-shifting phenomenon in a way that allows the analysis of future scenarios. If the past is any indication, the pace of technological change will outpace society's ability to appropriately defend against the risks of digitization unless researchers are able to shift from backwards-looking work to the evaluation of futures. Governments appear to be increasingly grappling with the results of decades of unfettered information-rights grabbing by international technology giants, but efforts to restore individual choices surrounding one's information in the digital realm will only chip away at these accumulated advantages and be vulnerable to new methods of accumulation without research paradigms that envision these consequences before they are actualized.

The ever-changing boundaries of privacy are a feature of the proposed framework, as each new technology or frontier artifact is initially conceptualized in terms of the distribution of rights it bestows and to whom it bestows them. In prior frameworks, each new frontier technology, such as illness detecting odor sensors, present new privacy pressures and concerns that need to be accounted for and researched in detail, often absent any larger societal context. In the proposed framework, this new technology is framed initially in terms of distribution of rights - it does not expand the size of overall rights, but instead represents a redistribution of rights within it. In the odor sensor example, instead of your health status existing as private information that you are free to choose to disclose, that right has been implicitly bestowed upon the purveyor of this technology. It is consideration of examples like this that the proposed framework attempts to explore.

Operationalizing the framework

In order to evaluate the proposed framework, it was necessary to construct a model through which it can be evaluated. Existing literature and refined models were used as the starting point, specifically the constructs that appear in the enhanced APCO model (Dinev et al 2015). Factors such as an individual's privacy concerns and threat perceptions, cultural and societal differences, and behavioral intentions were all deemed essential in operationalizing the proposed framework.

In considering how to proceed from those constructs to formation of a new model, the following overarching question was used:

> *How do future changes (artifacts, technologies, regulation) impact the (perceived) distribution of rights, and how would individuals perceive and respond to them?*

Considering the question above necessitated the development of new concepts and constructs, which included representation of the existing (equilibrium) distribution of decision rights, regulatory frameworks and dispositions (effectiveness of regulations), and some agent of change (technological artifact, vignette, etc.) that would be expected to affect the distribution of decision rights. This research opted for the use of vignettes through which to evaluate potential changes, consistent with the prior justification for new modes of speculative research put forth (Hovorka and Peter, 2021). It is important to note that although the development of specific technological artifacts remains an equally valid method of operationalization, it was not used for the current research and is something that could be explored in the future.

Research Questions

Evaluation of the new framework centers around the insights it can offer that that traditional user-agency centric frameworks cannot. Considering the previous question about how future changes impact distribution rights and individual responses, the following areas of evaluation are proposed:

(i) the nature of perceived threats (from which actor are threats most acute)

(ii) the viability of the vignettes as a research tool

(iii) the impact of different decision rights scenarios (vignettes) on outcomes (behavioral intention, desire for privacy and anonymity)

(iv) the role of changes to the distribution of decision rights in the impact of vignettes on outcomes

The development of research questions and hypotheses based upon these areas of investigation is discussed below.

The nature of perceived threats

The enhanced APCO model includes as antecedents to privacy concerns items such as privacy experiences and cultural and climate factors (Dinev et al 2015). In evaluating a model that frames the distribution of information rights as more than an antecedent, it is important to evaluate the relationship between factors such as societal attitudes, regulatory environment, privacy concerns and the distribution of decision rights and perceived privacy threats. Therefore, the following research question is posed:

RQ1: How do individual privacy concerns, regulatory environment, and societal values affect an individual's threat perception?

The following hypotheses were developed to address RQ1:

H1: Societal attitudes and regulatory environment will have a significant impact on an individual's initial threat perception.

H2: Societal attitudes, regulatory environment, and the distribution of information decision rights will have a direct effect on an individual's threat perception.

The viability of vignettes as a research tool

While the use of vignettes as a research tool were justified based on theory earlier, it remains an open question as to whether they are valid in this setting for this research project. Specifically, responses must be assessed for consistency, and certain trends are expected to emerge. To address this, the following research question is considered:

RQ2: How predictable are the changes to decision rights based on the vignettes?

In order to respond to RQ2, the following hypotheses were developed:

H3: Individuals will correctly identify who benefits (gains decision rights) in each vignette.

H4: The actor (group) assigned the primary decision rights in each vignette will see an increase in their share of decision rights.

H5: Actors not assigned the primary decision rights will see either no change or a decrease in decision rights (in other words, only one actor will see an increase in decision rights within any given vignette).

The impact of different decision rights scenarios (vignettes) on outcomes (behavioral intention, desire for privacy and anonymity)

This area is essentially already formatted as a research question, and involves evaluating the impact that the vignettes have on an individuals desire for privacy and anonymity as well as their anticipated behavioral response.

RQ3: How do the various decision rights scenarios (vignettes) affect outcomes?

The following hypothesis was developed:

H6: An individual's desire for privacy, anonymity, and expected behavioral responses will be affected by the type of actor (group) that gains decision rights.

The role of changes to the distribution of decision rights in the impact of vignettes on outcomes

In evaluating the role that decision rights play in an individual's desires and reactions regarding technology, the following research question was developed:

RQ4: How do changes in decision rights as a result of the vignettes affect outcomes?

This differs from the scenario presented in RQ3 in that it adds the change in decision rights; RQ3 (and H6) do not make use of the change in decision rights, rather they presume that simply identifying the actor that is perceived to gain decision rights will impact the outcomes. If the changes to decision rights are demonstrated to have an impact on outcomes, then the current operationalization of the decision rights-based framework will have been shown to describe a previously undescribed aspect of digital information privacy. Therefore, the following hypothesis was developed:

H7: Changes to decision rights will directly affect outcomes.

Chapter 4: Research Methodology

Chapter Three outlined the framework to be implemented and developed research questions and hypotheses to test an operationalization of the framework. This chapter elaborates on the methods used to collect data and the approach and techniques used to analyze the data.

Research Context

The project sought to consolidate privacy research across fields and develop a framework through which to assess technologies prior to implementation based upon the multi-level nature of privacy. It then sought to test this framework via the collection of survey data representative of different countries in order to make comparisons across a variety of societal and regulatory conditions. In order to gain information across countries, international students studying in the United States were sought. Survey recruitment took place across three phases, with participants of each phase being university students.

Methods of surveying existing privacy research

Seminal works published in MISQ in 2011 established the state of privacy research in IS at that time, and the current work appraised the progress made on questions raised at that time over the last ten years (2012-present). The current research integrates recent shifts towards more expansive elements of theorizing along with contributions from other disciplines, embracing imagined futures and their associated privacy impacts and drawing inspiration from the March 2021 MISQ special issue regarding next generation theorizing (see Burton et al 2021 for an introduction to the issue).

Literature searches were done first in the SSB8 from 2000 to present, with a set of identified keywords (privacy, anonymity, decentralized, centralized, distributed, security, secrecy, and confidentiality). Additional keywords were added based on appearance in the literature as well as outside readings (censorship, darknet or "dark web", co-option, surveillance, and data economy). The initial searches identified a 2011 MISQ special issue on privacy, which served as a delineation point along the 2000-2021 timeframe with which to assess progress. SSB8 papers from 2012 forward were reviewed in the context of the 2011 articles. Searches outside the SSB8 were conducted for terms related to privacy insufficiently covered in the primary stream of IS privacy research, as well as further back in time to trace the evolution of privacy across fields. Readings about privacy-related topics in the news or other well-circulated works on similar topics, such as Zuboff's article re: 'Big Other' and surveillance capitalism (preceded her recent book) as well as other frontier concerns were used to augment discussion and aid in speculating about the future of privacy and contributed to development of the framework.

Constructs of interest and survey development

As the most expansive and inclusive privacy framework in IS, the enhanced APCO model contains a number of constructs that are of interest in the current research. Privacy concerns and behavior (or intentions) are central to an analysis of privacy, and therefore remain in the models used in this research. Culture/Society is also an important construct that is utilized here (although instead of acting as an antecedent on privacy concerns it is expanded here alongside other constructs as having a potential direct impact on outcomes).

While keeping much of the existing expanded APCO model, constructs not specifically named above were not utilized in the current research due to differences in the foundational frameworks. Where the focus of APCO is solely on the individual, the framework outlined here includes additional group level actors like government and corporations and therefore requires a modified approach. APCO constructs specifically related to individual idiosyncrasies, primarily those concerned with the individual privacy calculus, were not used due to the adjusted scope.

New constructs were developed to account for the role that the distribution of decision rights occupies with respect to information privacy. Based on the ideas that it is not just the individual that exercises choice and that there are a number of external constraints operating on any actor regarding information privacy and decisional choice, a measure of decision right distribution was developed. Existing models filter everything through the individual and only attempt to measure variables that are entirely contained within an induvial by situating all external factors, where accounted for, as antecedents of individual privacy concerns. In order to make a privacy decision there has to exist meaningful choice, and the idea of decision rights that exist outside of an individual's conception of them is important to account for if privacy research in IS wants to build effective models in concert with other fields and expand its reach and relevance.

Another key consideration in the interaction among individuals, corporations, governments and other societal actors (NGOs, etc.) is the regulatory framework that exists. Regulatory framework here is defined as the norms in a society surrounding the rule of law, and is not a comparison of specific legislation and regulations that exist among countries. This decision was made due to the more aggregate-level focus on the distribution of rights - as the framework is focused on changes to existing equilibria, it is critical to have a conception of regulation that is more expansive and fluid. In fact, one of the vignettes (discussed in greater detail later) concerns new regulations, and by utilizing a regulatory construct focused on regulatory norms and enforcement, it allows for an exploration of specific regulatory changes and the anticipated impact based on the overall regulatory environment.

To summarize, five key constructs were identified for measurement: Individual Privacy Concerns (including privacy and anonymity), Regulatory Environment (Country of Citizenship), Societal Attitudes

(Country of Citizenship), Distribution of Decision Rights (Country of Citizenship), and Outcomes (behavioral intentions and privacy/anonymity desire). For a summary of how these constructs compare to those in the enhanced APCO model, refer to Table 4.1 below.

Table 4.1. Enhanced APCO Constructs

Construct	*Used*	*Not Used*	*New (not in APCO)*
Antecedent: Privacy Experiences/ Awareness	Somewhat (via threat perception)		
Antecedent: Personality/ Demographic		X (kept only Country of Citizenship)	
Antecedent: Culture/ Climate	X		
Trust		X (individual privacy calculus)	
Privacy Concerns	X		
Risk/costs		X (individual privacy calculus)	
Benefits		X (individual privacy calculus)	
Level of Effort		X	
Affect, Cognitive resources, time constraints		X	
Peripheral cues, biases, heuristics, misattribution		X (individual privacy calculus)	
Behavioral Reactions	X		
Regulatory Environment			X
Distribution of Decision Rights			X

Operationalization of the key constructs within the survey instrument resulted in a survey instrument with five main sections, with some additional demographic questions. The survey was divided into the following sections:

- Section 1: Privacy
- Section 2: Privacy and anonymity
- Section 3: Regulatory Environment
- Section 4: Societal Attitudes and Structures (includes distribution of decision rights)
- Section 5: Vignettes (includes outcome variables)
- Demographic questions

Each of the above sections are discussed further to provide information as to what was included in each.

Survey section 1: Privacy. This section covered individual privacy concerns and consisted of items developed specifically for this survey as well as nine items adapted from prior privacy research (Masur 2018, Baruh 2014). This includes items measuring privacy and anonymity concerns, overall privacy concerns, and concern based on the type of information.

Survey section 2: Privacy and anonymity. These items were developed for this survey, consisting of one likert question with seven items that sought to measure preferences for either privacy or anonymity with respect to different actors.

Survey section 3: Regulatory Environment. Regulatory environment was measured using items developed for this survey, and consisted of four items measuring the strength of regulation within an individual's Country of Citizenship.

Survey section 4: Societal Attitudes and Structures. This section covered societal attitudes, the distribution of decision rights, and perceived threat broken out by actor/group (individuals, corporations, government, community organizations, other) based on an individual's Country of Citizenship. Societal attitudes can be broken down into three sub-constructs: cultural orientation, individualist vs. collectivist disposition, and concentration of power. Cultural orientation consisted of four items adapted from

Hofstede's VSM 2013, disposition made use of three items developed for this survey, and concentration of power used a single item developed for this survey (Hofstede 2013). The distribution of decision rights item was developed for this survey and was the most challenging to implement. Inquiring about the distribution for a single country (Citizenship Country) helped focus this item, and the results will evaluate the ability to measure this construct. Perceived threat consisted of a single question with five items (one for each actor/group listed above).

Survey section 5: Vignettes. Outcome variables were operationalized through a series of vignettes containing four near-future scenarios that explore the impact of changes on an individual's desire for privacy and anonymity, expected behavioral response, nature of perceived threats to privacy, and the impact to the existing equilibrium of distribution of information rights. The four vignettes along with follow-up questions (same 6 question after each) were developed for use in this instrument, with one of the questions utilizing the concern scale found in Masur 2018 to allow for direct comparisons. The vignettes were developed to represent four unique scenarios, each involving an imagined increase or decrease in decision rights for a specific actor. The four scenarios represented included: (1) information centralization on behalf of the government to represent an increase in government decision rights, (2) novel technology implemented that increases corporate decision rights, (3) corporate charter amendments that increase an individual's decision rights, and (4) government requirements on data infrastructure that transfer rights from corporations to government. Inspiration for the vignettes was taken from recent headlines and anticipated changes in areas under development. Each respondent was presented with all four vignettes.

Demographic questions. The additional questions included Country of Citizenship, number of years lived in that country along with sense of connection to their Country of Citizenship, age, and gender.

Table 4.2 below lists the survey items and the construct they belong to for sections 1-4 (non-vignette questions, five total constructs):

Table 4.2. Survey items, sections 1-4 (non-vignette)

Item Abbreviation	*Construct*	*Measurement*

Privconc_overall	IPC (individual privacy concerns)	Likert-7
Pc1_Mas_v1	IPC	Likert-7
Pc1_Mas_v2	IPC	Likert-7
Pc1_Mas_v3	IPC	Likert-7
Pc_6	IPC	Likert-7
Pc1_Mas_v4	IPC	Likert-7
Pc1_Mas_v5	IPC	Likert-7
Pc_7	IPC	Likert-7
Pc_8	IPC	Likert-7
Cocit_reg1	REG (regulatory envt., country of Cit.)	Likert-5
Cocit_reg3	REG	Likert-5
Cocit_reg4	REG	Likert-5
Cocit_reg5	REG	Likert-5
Cocit_hof_soc_1	SOC (societal attitude: individual/collective disposition, Country of Cit.)	Likert-5
cocit_hof_soc_2.R	SOC	Likert-5
cocit_hof_soc_3	SOC	Likert-5
cocit_hof_soc_4.R	SOC	Likert-5
cocit_soc1	SOC	Likert-5
cocit_soc2.R	SOC	Likert-5
cocit_soc3	SOC	Likert-5
cocit_soc4.R	SOC (concentration of power)	Likert-5
cocit_distr_decRts_1	DoR (Distribution of Rights, Country of Cit.)	Integer, 0-100
cocit_distr_decRts_2	DoR	Integer, 0-100
cocit_distr_decRts_3	DoR	Integer, 0-100
cocit_distr_decRts_4	DoR	Integer, 0-100
cocit_threat_1	PThr (Perceived threat, Country of Cit.)	Likert-7
cocit_threat_2	PThr	Likert-7
cocit_threat_3	PThr	Likert-7
cocit_threat_4	PThr	Likert-7

Table 4.3 below lists the survey items and constructs for survey section 5 (the four vignettes). Note that each item listed below appeared as four questions in the survey – once for each of the four vignettes. Each respondent was able to respond to each of the four vignettes. To illustrate, v_entity represents the following four survey questions: v1_entity, v2_entity, v3_entity, and v4_entity. They are listed once for brevity, the full survey instrument is available in Appendix A.

Table 4.3. Survey items, section 5 (vignettes)

Item Abbreviation	*Construct*	*Measurement*
v_entity	Entity	Multiple Choice (select one)
v_distrChg_1	DRChg (change in decision rights)	Likert-7
v_distrChg_2	DRChg	Likert-7
v_distrChg_3	DRChg	Likert-7
v_distrChg_4	DRChg	Likert-7
v_behavior_1	BI (behavioral intentions)	Yes/No
v_behavior_2	BI	Yes/No
v_behavior_3	BI	Yes/No
v_behavior_6	BI	Yes/No
v_behavior_5	BI	Yes/No
v_privDesire	PADes (Privacy & Anonymity Desire)	Likert-7
v_anonDesire	PADes	Likert-7

Data Collection

The previous section outlined the survey development and items included in the survey. This section discusses how the survey was advertised and how responses were collected. Survey responses were collected via an online survey platform (Qualtrics).

Sampling and Recruitment. Sampling was intended to represent individuals across countries in order to obtain information on differing decision right distribution schemes, societal attitudes, and regulatory structures. Given the researcher's lack of direct access to international audiences and lack of resources to support widespread distribution of the survey in multiple languages, international students studying in the US were used to represent international perspectives, with the information on the various countries coming from these students' Country of Citizenship. In addition to the sampling of international students, responses were collected from US university students studying information systems and technology to allow for some comparison between US and international results.

The survey instrument was originally distributed to international students at three US universities (one graduate-only, two undergraduate universities) in October 2022 via email from the university International Student Offices. The same instrument was then distributed using an anonymous link in November 2022 via the following social media platforms: a discord server for international students, as well as a reddit group devoted to international students studying in the United States. In order to determine the source of a particular response (to distinguish between these two samples), a copy of the survey instrument was used with a different link. After these distributions, in an effort to increase the number of responses, a third distribution was sent to obtain responses from domestic students. This third survey was distributed to all students studying Information Systems at a US graduate university in February 2023. Given that domestic or international students could respond to this third survey, the instrument was modified slightly to rephrase the country and citizenship questions to accommodate domestic respondents, as well as moved these questions to the beginning of the survey to prevent response data being collected without knowing whether it was an international or domestic respondent. All construct-related items and scales remained identical to the prior versions. Table 4.4 below shows the number of responses for each of the three distribution channels:

Table 4.4. Response count by distribution method

Distribution method	*Distribution Date(s)*	*Surveys started*	*Completed 85% of non-vignette questions*	*Completed at least one vignette*
International students, three universities	10/17/2022, 11/16/2022, 11/29/2022	52	21	17

Social Media (Discord, Reddit)	10/30/2022, 11/4/2022	5	1	1
Information Systems students, one university	2/7/2023	19	10	10
Totals		76	32	28

After collection, responses were evaluated for inclusion using the following criteria: percentage of the survey completed (number of questions seen), number of items responded to (response density), and a scan for valid data patterns. Valid data patterns include the time it took respondents to complete the survey as well as a review of consecutive item responses. For example, there was a response that had 'strongly agree' selected regardless of prompt, the number of consecutive same responses regardless of prompt indicated an invalid response and this response was removed from the data prior to analysis. Additionally, any response with a completion time of less than seven minutes was deemed invalid as one could not be expected to complete the survey in this amount of time with a reasonable amount of thought and effort put forth. This amount of time was based on the survey length and repeated testing and passes through the survey (specific time estimated were provided to respondents for each survey section).

When considering responses for inclusion, a distinction was made between the vignette portion of the survey and the remainder of the survey (non-vignette portion) due to the nature of the analyses - some hypotheses only concerned the non-vignette sections. The threshold for inclusion for the non-vignette sections was set at 85%, representing broad coverage of these items. For the vignettes, initial screening used a threshold of 70%, with final cleaning ensuring that only vignettes with valid and complete responses were included in the relevant analyses as these sections contained outcome variables. Note that the vignettes were each independent of each other, and for the vignette analysis these responses were converted to a vertical (stacked) form rather than the original wide format where a single response contained four vignette responses. There was one respondent who responded to vignette #1 in its entirety and no others, and another that had a valid response pattern for vignette #1 but decided to fill out all remaining three vignettes with the same exact numerical response. In both cases, only valid responses were carried over into the final vertical data set for analysis. This resulted in 28 valid responses for vignette #1, and 26 valid responses each for vignette #2, vignette #3, and vignette #4.

Analysis

The R statistical programming language was used for analysis of the survey data. The initial plan was to compare differences across countries, however due to the relatively low number of responses received this was not feasible.

The survey constructs of interest are Individual Privacy Concerns, Regulatory Environment, Societal Attitudes, Distribution of Rights, Perceived Threat, primary entity (group) gaining decision rights in each vignette, the Change in Decision Rights, Behavioral Intentions, and Privacy/Anonymity Desire.

Table 4.5 outlines the constructs included in the analyses:

Table 4.5. Constructs and data collected

Construct Abbreviation	*Construct Description*	*Construct Type*	*Vignette Section*
IPC	Individual Privacy Concerns	Reflective	
REG	Regulatory Environment	Reflective	
SOC	Societal Attitudes	Reflective	
DoR	Distribution of Rights	Composite Categorical, Single-item	
PThr	Perceived Threat Actors	Reflective	
Entity	The vignette entity gaining decision rights	Formative (Composite Categorical)	Yes
DRChg	Change in Decision Rights – gain or loss by Actor/Group	Single Item	Yes
BI	Behavioral Intention	Single Item	Yes
PADes	Privacy & Anonymity Desire	Reflective	Yes

Chapter 3 outlined the hypotheses, and the following section outlines the methods by which they will be examined using the constructs identified. RQ1 and RQ2 are simpler and more foundational, with RQ1 attempting to distinguish that regulatory environment, social attitudes, and distribution of decision rights are more than antecedents and have a role outside an individual's perceptions, while RQ2 involves validating decision rights as a measurable concept. RQ3 and RQ4 aim to test the impact of future imagined scenarios on the outcome variables and validate the framework as a plausible option for future privacy research.

(H1) Societal attitudes and regulatory environment will have a significant impact on an individual's initial threat perception. This hypothesis made use of the REG, SOC, and PThr constructs. Each of these constructs was composed of multiple likert items, and ordinary least squares regression was used to assess the impact of REG and SOC on PThr. In order to analyze these constructs using a regression model, the construct items were first converted into composite variables. Cronbach's alpha was used to assess the internal consistency reliability of the items prior to the creation of the composite items. The regression equation used was:

$$\text{REG} + \text{SOC} = \text{PThr}$$

Analyses were run using the R statistical programming language, with Cronbach's alpha calculated using the psych package and regressions calculated using the base R functionality (Revelle 2023, R Core Team 2021).

(H2) Societal attitudes, regulatory environment, and the distribution of information decision rights will have a direct effect on an individual's threat perception. This hypothesis made use of the REG, SOC, DoR, and PThr constructs. Similar to H1, H2 utilized ordinary least squares regression to assess the impact of REG, SOC, and DoR on PThr. Cronbach's alpha was used to develop composite measures for all but one of these constructs, DoR, for the evaluation of H1 as outlined in (Caughlin 2022). DoR was measured in the survey as integers (summed to 100) for each of the entities and their share of decision rights. There were four entities listed for the sake of broad coverage, however only three received ratings in the responses; individuals, government, and corporations all had ratings while NGO's received no numeric ratings by any respondent. Due to the measurement of this variable, different approaches were utilized. Raw integer values were used but were deemed insufficient as each response contained three individual values that combined represented a particular pattern beyond the individual scores. Four regimes were identified: highly concentrated regimes where one entity had 55% or greater of decision rights and one entity had 10% or less, dominant regimes where one entity had 50% or greater share and each entity had greater than 10%, balanced regimes where no entity had more than 48% share or less than 20% share, and a final regime that encapsulated all other cases such as dual-dominant or equal-spacing hierarchical distributions. These four regimes were coded as three dummy variables for inclusion in the regression model. Beyond the use of the raw values and the dummy variables representing regimes, a single binary variable was created to differentiate regimes based on the share that went to individuals, with 30% being the chosen cutoff point (the mean share reported for individuals was 28.6%) to represent regimes that were favorable to individuals. The regression equations used are shown below:

a) REG + SOC + DoR(Indiv) + DoR(Corp) + DoR(Govt) = PThr

b) REG + SOC + Dummy(Conc) + Dummy(Dom) + Dummy(Bal) = PThr

c) REG + SOC + Dummy(Indiv) = PThr

Calculations were done as described above in H1.

(H3) Individuals will correctly identify who benefits (gains decision rights) in each vignette. The evaluation of this hypothesis made use of the ENTITY construct, along with the researcher-designated entity (or group). Each vignette describes a scenario in which at least one actor (group) gains decision rights, and this hypothesis involved a comparison of the entity gaining decision rights within each vignette as identified by respondents with the entity identified by the researcher. A simple percentage of respondents able to correctly identify the primary actor gaining rights is sufficient to determine if identification by respondents was successful and can speak to whether the concept of decision right attribution appears measurable by the instrument used. This was the first hypothesis to make use of variables from the vignette section of the survey and was structured differently. The non-vignette sections had 34 responses, as described previously (Table 4.2). For the vignette section, each respondent was presented with four different scenarios, and therefore the data for H3 and the subsequent vignette-related hypotheses hade use of stacked data, where each respondent had an observation for each of their vignette responses. This resulted in 105 valid observations.

(H4) The actor (group) assigned the primary decision rights in each vignette will see an increase in their share of decision rights. The evaluation of this hypothesis involved the Entity and DRChg constructs, and utilized mean and frequency tables to observe whether the entity identified by respondents had in increase in the share of decision rights.

(H5). Actors not assigned the primary decision rights will see either no change or a decrease in decision rights. The evaluation of this hypothesis used the ENTITY and DRChg constructs and involved mean calculations and ANOVA analysis to determine if there were statistical differences between the respondent identified entity decision rights and other entity decision rights as a result of each vignette. Each self-identified entity was examined individually, so there was an analysis done for each of the cases where individuals, corporations, governments, and NGOs were identified as the primary entity gaining decision rights. Post-hoc testing was done using Dunnett's test to compare the selected group against all others and calculated in the R statistical programming language using the multcomp package as outlined by Antoine Soetewey in 2020 (Soetewey 2020, Hothorn et al 2008).

(H6). An individual's desire for privacy, anonymity, and expected behavioral responses will be affected by the type of actor (group) that gains decision rights. The evaluation of this hypothesis involved the use of the ENTITY, IPC, REG, SOC, and BI constructs. In determining the effect of the self-reported entity on behavioral intention, it is hypothesized that the regulatory, individual privacy concern, and societal constructs affect this relationship. In order to test and model these effects, PLS-SEM was selected for a variety of reasons: the utility such models in assessing moderating relationships, the effectiveness of the statistical techniques with smaller sample sizes, and the ability of the technique to effectively model complex interactions (Hair et al 2017). The constructs IPC, REG, and SOC are all composite reflective constructs. BI is a single-item construct. The ENTITY construct was measured in the survey as a single self-reported response (i.e. "which entity is the primary entity gaining decision rights in the scenario described"). In order to be used in the PLS-SEM model, the survey item was converted into four dummy variables. The use of this new composite categorical construct followed the procedures outlined in Hair et al (Hair et al 2019). The data was standardized following procedures outlined by Lohmoller, and evaluated to ensure that it met the necessary criteria (Lohmoller 1989). The statistical analysis and evaluation of validity and reliability for the model follow the procedures outlined by Hair et al 2021, and used the SEMinR package in the R statistical programming language (Ray and Danks 2021). The structural model analyzed is shown below in Figure 4.1:

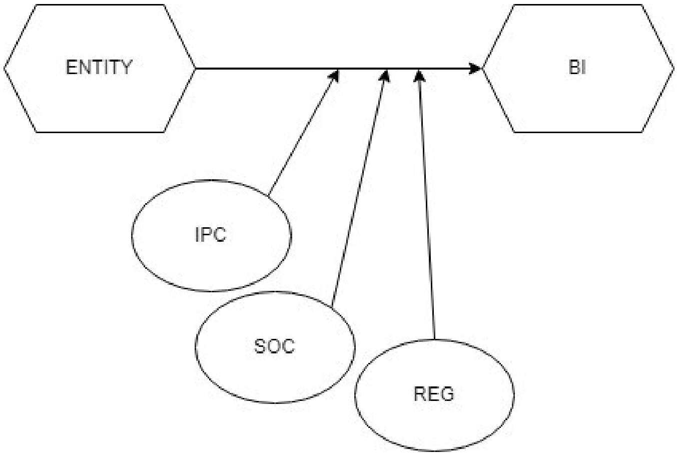

Figure 4.1. H6 structural model

(H7). Changes to decision rights will directly affect outcomes. The evaluation of this hypothesis involved the use of the ENTITY, IPC, REG, SOC, DRChg, and BI constructs. The only additional construct in H7 not found in H6 is the DRChg construct. This construct was measured in the survey via a multi-item likert question, with each entity (individual, government, corporation, NGO) being a distinct item measured on a 7-point scale with the midpoint, the fourth scale item, representing no change in rights for that entity. In order to utilize this data in the model, responses were transformed into a single measure that was defined as the absolute change in decision rights. This absolute change was calculated as the sum of the absolute value of each entity's change from the midpoint (no change). To illustrate, consider a respondent that indicated the following changes to decision rights as a result of the scenario: significant increase for individuals, significant decreases for both government and corporations, and no change for NGOs. The numerical values (on a 1 to 7 scale, with 4 representing no change) would be a 7 for individuals, 1 for government and 1 for corporations, and 4 for NGOs. Taking the absolute value of the difference from 4 (the middle no change anchor point) of each of those scores and summing them yields the total change in decision rights as a result of the vignette, in the sample case presented it would be 9. While the DRChg construct was added in the H7 model, the nature of the relationships was also changed from H6 in order to assess whether the DRChg construct was (a) affected by the ENTITY construct and (b) if the DRChg construct affected the BI directly. The structural model for H7 is shown below:

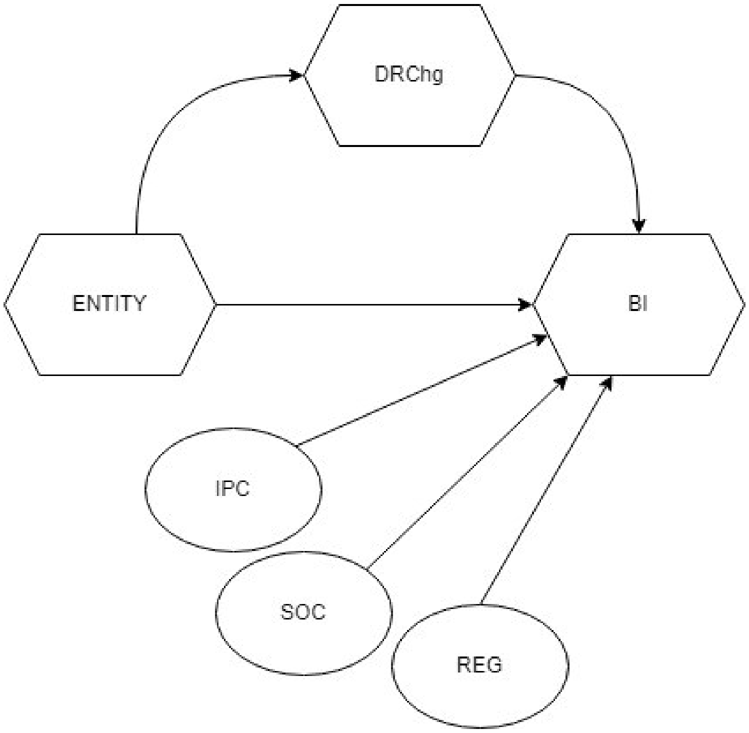

Figure 4.2. H7 structural model

Notice that the DRChg construct is introduced as an intermediate construct that is affected by the ENTITY construct and affects the BI (outcome) construct.

Analysis of H7 using PLS-SEM was conducted as in H6, using the R package SEMinR and following Hair et al 2021. A summary of the hypotheses along with relevant constructs and methods of analysis are presented in Table 4.6 below:

Table 4.6. Hypotheses and analysis methods

H	*Hypothesis*	*Method of Analysis*	*Constructs*	*RQ*

H1	Societal attitudes and regulatory environment will have a significant impact on an individual's initial threat perception	OLS regression (SOC, REG as independent vars; PThr as dependent var)	SOC, REG, PThr	RQ1
H2	Societal attitudes, regulatory environment, and the distribution of information decision rights will have a direct effect on an individual's threat perception	OLS regression (SOC, REG, DoR as independent vars; PThr as dependent var)	SOC, REG, DoR, PThr	RQ1
H3	Individuals will correctly identify who benefits (gains decision rights) in each vignette	Ratio (researcher/respondent match rate)	ENTITY	RQ2
H4	The entity (group) assigned the primary decision rights in each vignette will see an increase in their share of decision rights	Basic descriptives	ENTITY, DRChg	RQ2
H5	Entities (groups) not assigned the primary decision rights will see either no change or a decrease in decision rights	Basic descriptives, ANOVA, post-hoc analysis (Dunnett's test)	ENTITY, DRChg	RQ2
H6	An individual's desire for privacy, anonymity, and expected behavioral responses will be affected by the type of entity (group) that gains decision rights	PLS-SEM	ENTITY, IPC, REG, SOC, BI	RQ3
H7	Changes to decision rights will directly affect outcomes.	PLS-SEM	ENTITY, IPC, REG, SOC, BI, DRChg	RQ4

Basic Demographic Summary of Survey Responses

The tables below present basic demographic information collected from survey respondents. The results are inclusive of all distribution channels. Table 4.7 below presents the responses by US citizenship:

Table 4.7. Responses by US Citizenship

US Citizen	*Count*	*%*	*Mean # of years in Country of Citizenship*	*Mean, Overall Privacy Concern (1 to 7)*
Yes	6	19%	22	4.70
No	23	72%	25.6	4.67
Unknown	3	9%	NA (not reported)	3.67

	4.59

From Table 4.7 above, respondents were more likely to be non-US citizens at roughly a 3 to 1 ratio. The mean number of years respondents have lived in their Country of Citizenship were roughly the same when comparing US to non-US respondents, and the mean level of overall privacy concerns was roughly equal amongst those two groups (with those not reporting country information at a lower level of overall concern).

Table 4.8 below summarizes responses by geographic region:

Table 4.8. Responses by region

Geographic Region	*Count*	*%*	*Mean, Overall Privacy Concern (1 to 7)*
Africa	4	13%	6.25
Asia	7	22%	5.00
Europe	3	9%	2.67
Middle East	5	16%	4.40
North America	6	19%	4.67
South America	2	6%	4.00
Unknown	5	16%	4.20
			4.59

From Table 4.8 above, the respondents were distributed across a number of regions, and there were differing levels of concern apparent amongst the continents. Respondents that were citizens of an African nation or Asian nation were the most concerned about information privacy, followed by citizens of North American, Middle Eastern and South American countries, with European citizens reporting the least concerns by a wide margin. This is not surprising given the recent focus of EU nations on protecting individual privacy.

Responses by age and gender are reported below in Tables 4.9 and 4.10, respectively:

Table 4.9. Responses by gender

Sex	*Count*	*%*	*Mean, Overall Privacy Concern (1 to 7)*
Female	14	44%	3.93
Male	14	44%	5.36
Unknown	4	12%	4.25
			4.59

Table 4.10. Responses by age

Age	*Count*	*%*	*Mean, Overall Privacy Concern (1 to 7)*
24 or younger	4	13%	4.00
25-29	5	16%	4.00
30-34	5	16%	5.40
35-39	5	16%	4.20
40-49	4	13%	5.75
50-59	3	9%	5.67
60 or above	1	3%	3.00
Unknown	5	16%	4.00
			4.59

From Table 4.9 above, an equal number of male and female responses were received, with male respondents reporting a higher level of overall privacy concern.

Tables 4.11 through 4.14 (below) summarize the mean distribution changes in information decision rights reported for each of the four vignettes:

Table 4.11. Vignette #1 decision right changes

Entity / Group (self-reported)	*Count*	*Mean DR Change, Individuals*	*Mean DR Change, Corporations*	*Mean DR Change, Government*	*Mean DR Change, NGOs*
Corporations	1	4.00	4.00	4.00	4.00
Government	18	2.94	4.69	5.94	3.69
Individuals	6	3.33	4.17	5.83	4.00
NGOs	3	4.67	4.67	4.33	4.67
Totals	28	3.26	4.50	5.70	3.88

Table 4.12. Vignette #2 decision right changes

Entity / Group (self-reported)	*Count*	*Mean DR Change, Individuals*	*Mean DR Change, Corporations*	*Mean DR Change, Government*	*Mean DR Change, NGOs*
Corporations	5	4.20	5.80	4.20	4.20
Government	4	4.00	4.25	6.00	4.00
Individuals	17	5.41	4.47	4.00	4.24
NGOs	1	7.00	6.00	6.00	6.00
Totals	27	5.04	4.74	4.41	4.26

Table 4.13. Vignette #3 decision right changes

Entity / Group (self-reported)	*Count*	*Mean DR Change, Individuals*	*Mean DR Change, Corporations*	*Mean DR Change, Government*	*Mean DR Change, NGOs*
Corporations	7	3.29	5.43	3.86	4.00
Government	10	4.70	3.90	5.50	4.44
Individuals	8	4.88	5.00	5.25	4.50
NGOs	1	NA	NA	NA	7.00
Totals	26	4.35	4.77	4.92	4.42

Table 4.14. Vignette #4 decision right changes

Entity / Group (self-reported)	*Count*	*Mean DR Change, Individuals*	*Mean DR Change, Corporations*	*Mean DR Change, Government*	*Mean DR Change, NGOs*
Corporations	3	4.00	3.67	5.00	4.33
Government	19	3.58	3.63	6.16	4.18
Individuals	3	4.33	5.67	5.67	5.00
NGOs	1	7.00	1.00	1.00	7.00
Totals	26	3.85	3.77	5.77	4.42

Chapter 5: Results

This section presents the results of the analyses for hypotheses H1 through H7 according to the methodological processes outlined in the previous chapter.

H1: Societal attitudes and regulatory environment will have a significant impact on an individual's initial threat perception

H1 evaluated the effect that societal attitudes and regulatory environment have on an individual's perceived threat from various entities.

Analysis of H1 required the creation of composite variables for use in a regression equation. Assessment of item suitability for inclusion in composite variables was done using Cronbach's alpha, with computation in R using the psych package following procedures outlined in Caughlin 2022. Cronbach's alpha is a suitable choice as it can provide a measure of internal consistency reliability by determining if items within each construct reliably measure the same concept. Cronbach's alpha calculations were done for the IPC, REG, SOC, and PThr constructs using the widely established threshold of alpha = 0.70 or above for inclusion (Caughlin 2022).

IPC (Individual Privacy Concerns) was evaluated first, with an overall raw alpha of 0.90, and a standardized alpha of 0.89. The item ‘Q27.R’ was negatively correlated with the other items and the reliability if that item was dropped increased to 0.94, indicating that the overall reliability of the construct would improve were this item removed. Additionally, upon review of the specific items, this item (“Strong individual privacy rights are detrimental to public safety”) was conceptually distinct from the remainder of the items that asked about levels of concern related to information collection and use. Therefore, item ‘Q27.R’ (commitment to privacy) was dropped from the construct.

Running the Cronbach’s alpha with ‘Q27.R’ removed resulted in an alpha of 0.94 (raw and standardized). The results of the analysis for the IPC construct items are presented below:

Table 5.1. Cronbach’s alpha, IPC construct

IPC Construct							
Item	*n*	*raw.r*	*std.r*	*r.cor*	*r.drop*	*mean*	*sd*
privconc_overall	32	0.81	0.81	0.8	0.75	4.6	1.6
pc1_Mas_v1	32	0.82	0.82	0.82	0.76	5.1	1.5
pc2_Mas_v2	32	0.84	0.85	0.84	0.8	5.7	1.3
pc3_Mas_v3	32	0.83	0.83	0.81	0.77	5.3	1.6
pc6	32	0.82	0.83	0.81	0.78	5.6	1.4
pc4_Mas_v4	32	0.79	0.78	0.75	0.71	5.3	1.8
pc5_Mas_v5	32	0.79	0.79	0.77	0.73	5.2	1.4
pc_7	32	0.79	0.78	0.76	0.73	4.6	1.6
pc_8	32	0.86	0.85	0.84	0.81	5.4	1.5

With an overall alpha of 0.94 and each item having an alpha of 0.79 or above, above the 0.70 threshold, these 9 items were selected to comprise the IPC construct.

REG (regulatory environment) consisted of four items, with a raw alpha of 0.88 and a standardized alpha of 0.87. The results of the analysis for the REG construct items are presented below:

Table 5.2. Cronbach’s alpha, REG construct

REG *Construct* *Item*	*n*	*raw.r*	*std.r*	*r.cor*	*r.drop*	*mean*	*sd*
cocit_reg1	32	0.86	0.85	0.79	0.73	3.3	1.3
cocit_reg3	32	0.94	0.94	0.94	0.88	3	1.4
cocit_reg4	32	0.90	0.90	0.87	0.82	3	1.2
cocit_reg5	32	0.70	0.72	0.57	0.53	2.9	1.1

With an overall alpha of 0.88 and no item having an alpha less than 0.70, these four items were used to measure regulatory environment.

SOC (societal attitudes/disposition) initially consisted of eight items. The Cronbach's alpha for these eight items was 0.43 (standardized alpha was 0.41). Some of these items had negative correlations and were reversed, however the resulting raw alpha only improved to 0.50. As constructed, these eight items did not provide a consistent measure of the construct. Reviewing the content of these items, several of the items came from Hofstede's VSM and the others were developed for this survey. These two groups of items were split and Cronbach's alpha was calculated for each group, with neither having an alpha of greater than 0.70. A second review of item content was done, and the two items "cocit_soc1" and "cocit_soc3" ("society in my country of citizenship places a high priority on individual rights and freedoms" and "society in my country of citizenship places a high priority on ideas of ownership and private property"), respectively, appeared to best capture the core of what the construct was intended to represent – societal disposition regarding privacy-enabling foundations. Cronbach's alpha for these two items was 0.75 (standardized alpha = 0.76), and the reliability if either item was dropped went down and therefore these two items were chosen to represent the societal attitude construct.

Table 5.3. Cronbach's alpha, SOC construct (initial)

SOC Construct *Item*	*n*	*raw.r*	*std.r*	*r.cor*	*r.drop*	*mean*	*sd*
cocit_hof_soc_1	32	0.59	0.54	0.42	0.3035	3.7	1.25
cocit_hof_soc_2.R	32	0.21	0.31	0.17	-0.0081	1.5	0.84
cocit_hof_soc_3	32	0.29	0.37	0.23	0.0746	3.7	0.81
cocit_hof_soc_4.R	32	0.53	0.51	0.36	0.2704	2.2	1.12

cocit_soc1	32	0.6	0.55	0.57	0.3639	3.2	1.11
cocit_soc2.R	32	0.28	0.31	0.2	0.0327	2.6	0.95
cocit_soc3	32	0.5	0.52	0.5	0.2664	3.6	1.01
cocit_soc4.R	32	0.47	0.41	0.27	0.1576	2.2	1.26

Table 5.4. Cronbach's alpha, SOC construct (revised)

SOC *Construct* *Item*	*n*	*raw.r*	*std.r*	*r.cor*	*r.drop*	*mean*	*sd*
cocit_soc1	32	0.91	0.9	0.7	0.61	3.2	1.1
cocit_soc3	32	0.89	0.9	0.7	0.61	3.6	1

PThr (Perceived Threat) consisted of four items. The Cronbach's alpha for these items was 0.72 (raw and standardized), indicating that the items hang together enough (beyond the 0.70 criteria) to form a composite construct. The results for the alpha calculations for the PThr construct are presented below:

Table 5.5. Cronbach's alpha, PThr construct

PThr *Construct* *Items*	*n*	*raw.r*	*std.r*	*r.cor*	*r.drop*	*mean*	*sd*
cocit_threat_1	32	0.75	0.74	0.67	0.51	4	2.1
cocit_threat_2	32	0.81	0.8	0.72	0.62	4.7	1.9
cocit_threat_3	32	0.59	0.6	0.4	0.29	4.8	1.9
cocit_threat_4	31	0.79	0.8	0.71	0.62	3.4	1.8

Note that the item "cocit_threat_3" item had a raw alpha of 0.59, and a reliability if dropped estimate of 0.77 which is below the overall raw alpha of 0.72. In consideration of adjusting this composite construct, the survey question asked about perceived threats across differing entities and therefore omitting the perceived threat from government ("cocit_threat_3") would result in an incomplete representation of overall threat perception and thus all four items were kept. Additionally, when constructing a composite variable, any item with an individual loading above 0.40 where the overall alpha is above 0.70 requires a solid reason to justify its removal (Caughlin 2022).

The analysis above resulted in the identification of individual items to compose the composite constructs, and the composite values were calculated using the rowMeans() function in the R statistical programming environment, with NAs omitted from the calculation.

The next step in evaluating H1 was to perform a regression of (a) the dependent variable PThr (perceived threat) on the composite variables representing REG (regulatory environment) and SOC (societal attitudes), followed by (b) regression of the dependent variable IPC (individual privacy concerns) on REG and SOC.

Table 5.6. H1-a regression results

	Estimate	*Std. Error*	*t value*	*Pr(>|t|)*
(Intercept)	4.2324	1.0583	3.999	0.0004 ***
reg.c	-0.2149	0.2518	-0.854	0.4002
soc.c	0.1883	0.2925	0.644	0.5249

From the table above, the REG and SOC composite variables were not statistically significant in explaining the variance in PThr. The overall R-squared value of the model was 0.0289 with a residual standard error of 1.44 on 29 degrees of freedom. The F-statistic for the model was 0.4308 with a p-value of 0.6541, well above the threshold for significance (0.05 or below).

In addition to evaluating the impact of REG and SOC on PThr, the impact of REG and SOC on IPC was evaluated (H1b).

Table 5.7. H1-b regression results

	Estimate	*Std. Error*	*t value*	*Pr(>|t|)*
(Intercept)	5.002	0.918	5.449	< 0.0001 ***
reg.c	-0.1852	0.2184	-0.848	0.403

soc.c	0.2169	0.2537	0.855	0.4

The Table above shows the results of the model REG + SOC = IPC. Additionally, the R-squared was 0.0356 with a residual standard error of 1.25 on 29 degrees of freedom. The F-statistic was 0.5349 with a p-value of 0.5914. Similar to the results of H1A, REG and SOC did not have a statistically significant relationship with IPC.

Based upon the regression analyses presented above, H1 was Not Confirmed. Societal attitudes and regulatory environment did not have a significant effect on threat perception.

H2: Societal attitudes, regulatory environment, and the distribution of information decision rights will have a direct effect on an individual's threat perception

Similar to H1, H2 made use of the composite items REG, SOC, and PThr as discussed in H1. Regression Models for H2 followed the general format:

$$REG + SOC + DoR = PThr$$

The difference between H1 and H2 is the inclusion of the distribution of information decision rights (DoR) in the H2 model. The distribution of information rights survey item simply asked for a percentage distribution (0-100) for each entity (individuals, corporations, government, NGOs). Differing variables were used to represent the distribution of rights construct: raw numeric values, dummy variables representing different distribution regimes regardless of entity (based on overall distribution patterns), and a conceptualization centered around individuals. The three models representing the various representations of DoR are shown below (refer to the Analysis section of Chapter IV for further discussion):

Table 5.8. Distribution of Rights representation (used in H2)

H2 Model	*Description of DoR*	*Number of Variables*	*Type of variable*

(a)	Raw numeric values representing share of rights for each of 3 entities	3	Numeric
(b)	Regime-based dummy variables	3	Dummy (binary)
(c)	Individual-dominant vs. Corporate/Govt distributions	1	Dummy (binary)

The regression model for H2a is as follows:

H2(a): REG.c + SOC.c + Distr(Ind) + Distr(Corp) + Distr(Govt) = PThr.c

The resulting estimation of the model did not return a coefficient estimate for Distr(Govt) due to singularities, however the correlation matrix among all model variables did not yield any two variables with perfect (or near-perfect) correlations (see Appendix B for regression table and correlation values). The R-squared value for the model was 0.1242, with and F-statistic of 0.9573 and p-value of 0.4467 indicating that the model as specified did not have statistical explanatory value for the PThr construct.

H2b utilized three dummy variables to represent four distribution regimes (refer to the Analysis section of Chapter IV for further explanation):

H2(b): REG + SOC + Dummy(Conc) + Dummy(Dom) + Dummy(Bal) = PThr

Model H2(b) results are shown below:

Table 5.9. H2-b regression results

	Estimate	*Std. Error*	*t value*	*Pr(>|t|)*
(Intercept)	5.7987	1.3337	4.3480	0.0002***
distr_conc	-1.5804	0.7124	-2.2180	0.0355*
distr_dom	-1.6241	0.6214	-2.6140	0.0147*
distr_bal	-0.5575	0.8229	-0.6770	0.5041
reg.c	-0.1370	0.2480	-0.5530	0.5853
soc.c	-0.0489	0.2900	-0.1690	0.8675

The overall R-squared for model H2(b) was 0.273, with residual standard error of 1.319 on 26 degrees of freedom. The F-statistic was 1.953 with a p-value of 0.1196. From the regression results, both the "concentrated" and "dominant" regimes proved significantly related to the PThr at the alpha = 0.05 level. This indicated that respondents within a concentrated or dominant distribution regime, lower levels of perceived threat were reported (as measured as threat across all actors).

Model H2(c) made use of the model specified below:

H2(c): REG + SOC + Dummy(Indiv>=30%) = PThr

The results of model H2(c) are presented below:

Table 5.10. H2-c regression results

	Estimate	*Std. Error*	*t value*	*Pr(>|t|)*
(Intercept)	4.8903	1.0598	4.6140	0.0001***
distr_indiv	1.1420	0.5710	2.0000	0.0553 .
reg.c	-0.2873	0.2424	-1.1850	0.2459
soc.c	-0.0840	0.3100	-0.2710	0.7883

The overall R-squared for model H2(c) was 0.1502, with residual standard error of 1.374 on 28 degrees of freedom. The F-statistic was 1.65 with a p-value of 0.20. From the table above, the dummy individual-centric distribution regime variable was not quite significant at the 0.05 level (0.055), but was very close to that cutoff and indicative of a potential trend. This suggests that respondents in environments where individuals have a larger degree of decision rights relative to other actors generally report higher perceived threat levels (as represented by the mean threat level across the four main entities).

H1 indicated there was no significant relationship between REG and SOC and the PThr. H2 explored whether the addition of the distribution of rights (DoR) changed that conclusion and affected the

PThr. The results indicate that dependent upon the conceptualization of distribution or rights, that distribution can indeed impact the perceived threat levels of individuals. Note that this result was dependent upon exactly how the distribution of rights is specified, and did not hold for all cases, most notably the raw numeric distribution values provided by participants. As a result, H2 is suggested, but not entirely confirmed. Further analysis and exploration is necessary to confirm this relationship.

H3: Individuals will correctly identify who benefits (gains decision rights) in each vignette

The table below shows the frequency counts for the researcher-indicated entity gaining decision rights and the count of respondents indicating the entity gaining rights:

Table 5.11. Researcher vs. respondent identified entities gaining decision rights

Researcher-Identified Entity	*Respondent Entity - Corporations*	*Respondent Entity - Government*	*Respondent Entity - Individuals*	*Respondent Entity - NGOs*	*% Correctly identified*
Corporations	5	3	17	1	19%
Government	4	37	9	4	69%
Individuals	7	9	8	1	32%

The table above indicates different trends in terms of how well respondent identified entities gaining decision rights matched the researcher-assigned entity. In general, respondents were able to correctly determine when governments were gaining decision rights (69%), but far less able to determine when corporations or individuals were gaining rights (19% and 32%, respectively), often conflating the two. This contrast is particularly stark for the case of individuals; in the vignette designed to enhance corporate decision rights, over 65% of respondents indicated that individuals were the primary beneficiaries. In the vignette designed to enhance individual decision rights, 36% of respondents indicated that government was the primary beneficiary and another 28% that corporations were the primary beneficiary (with 32% correctly identifying individuals).

The vignettes included two vignettes where government was the primary beneficiary; in an effort to determine if the wording of the vignettes was primarily at play the two government vignettes were compared. Widely differing identification rates across the two government vignettes would indicate that the wording of the vignettes was the primary driving factor in the differences found between the government vignettes and the other vignettes whereas consistency amongst the two would suggest that there were actual observed differences between the government and other vignettes.

Table 5.12. Comparison of the two government vignettes (vignettes #1 and #4)

Entity reported to gain DR	*V1 (28 responses)*	*V4 (26 responses)*
Corporations	1	3
Government	18	19
Individuals	6	3
NGOs	3	1
% Correct	64%	73%

From the table above, the percentage of respondents able to correctly identify the correct entity gaining decision rights was comparable across the two government vignettes. The percentages correctly identified here are far closer than the difference between either government vignette and the other two vignettes, suggesting that there is a real difference in respondents' ability to determine a situation where the government gains decision rights compared to situations where individuals or corporations are gaining decision rights.

Thus, H3 is partially confirmed – respondents were able to correctly identify when governments gain decision rights but unable to reliably do so when either corporations or individuals are gaining decision rights.

H4: The entity (group) assigned the primary decision rights in each vignette will see an increase in their share of decision rights

H4 is evaluated in by looking at the reported decision right changes for the entity identified by the user as the primary entity gaining decision rights, organized by vignette. The tables below present the results:

Table 5.13. Self-identified entity change in decision rights, response counts

Vignette	*n =*	*Significant decrease (1)*	*2*	*3*	*No change (4)*	*5*	*6*	*Significant increase (7)*
v1	26	1	2	1	5	3	6	8
v2	26	0	2	1	3	2	11	7
v3	25	0	1	0	5	7	9	3
v4	26	0	2	1	1	4	9	9

Table 5.14. Self-identified entity change in decision rights, summary statistics

Vignette	*% Reporting an increase*	*Mean value*	*Std dev*
v1	65%	5.192	1.789
v2	77%	5.539	1.502
v3	76%	5.280	1.173
v4	85%	5.692	1.490

From the tables above, each entity that was identified as the primary entity gaining decision rights saw an increase in reported share of decision rights. This can be observed from both the percentages as well as the mean values, where a mean of 4.0 indicated no change for that entity in decision rights.

The overall mean for self-identified entities was 5.472 across all four vignettes, where 4.0 represents no change. Based on the results presented in this section, H4 is confirmed – the entity assigned primary decision rights reported gains in decision rights.

H5: Entities (groups) not assigned the primary decision rights will see either no change or a decrease in decision rights

H5 involved analysis of reported decision right changes for the self-identified primary entity versus the entities not identified as primary entities in order to determine if there were any significant differences. The first step in this analysis was creating variables that represent decision right changes for each entity when it was not selected as the primary entity. This was done for each entity: individuals, corporations, governments, and NGOs. The means of these variables were calculated and represent the means for entities that were not the self-identified primary entity. To illustrate, the mean value for government represents the mean government decision right change in situations where government was NOT selected as the primary entity. The mean decision right change for an entity when it was not selected versus when it was is shown below, along with results of Welch's t-test testing the hypotheses that the means between the two groups are zero (equal):

Table 5.15. Mean change in decision rights when NOT primary entity

Entity	*Mean when not selected as primary*	*Mean when primary*	*Welch's t statistic (sel vs. non-sel)*	*p-value*
Govt	4.536	5.896	-5.187	< 0.0001 ***
Indiv	3.700	4.824	-2.925	0.0046 **
Corp	4.264	5.125	-2.065	0.0505 .
NGO	4.095	6.000	-3.384	0.0234 *

To further describe each entity and the change in that entity's decision rights when varying entities were selected as the primary entity, a series of boxplots are presented below:

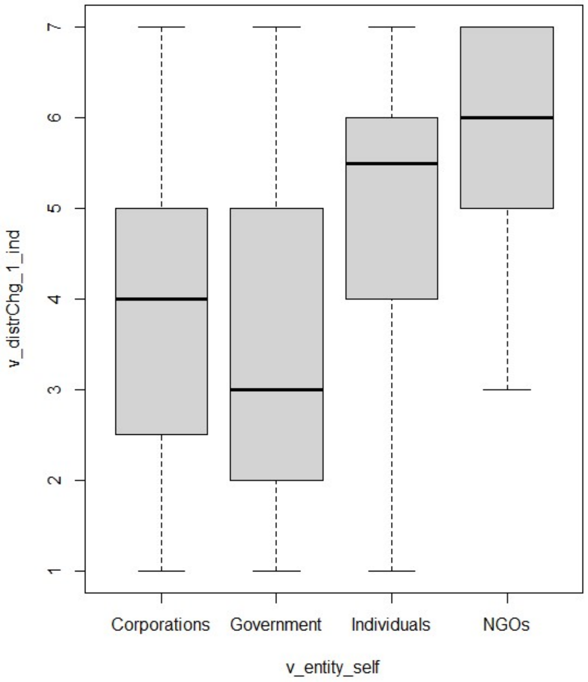

Figure 5.1. Boxplot, individuals' decision right change

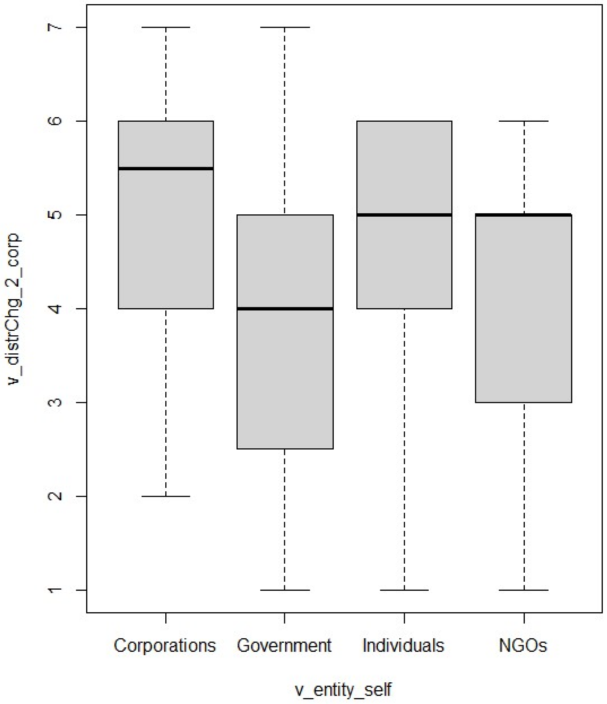

Figure 5.2. Boxplot, corporations' decision right change

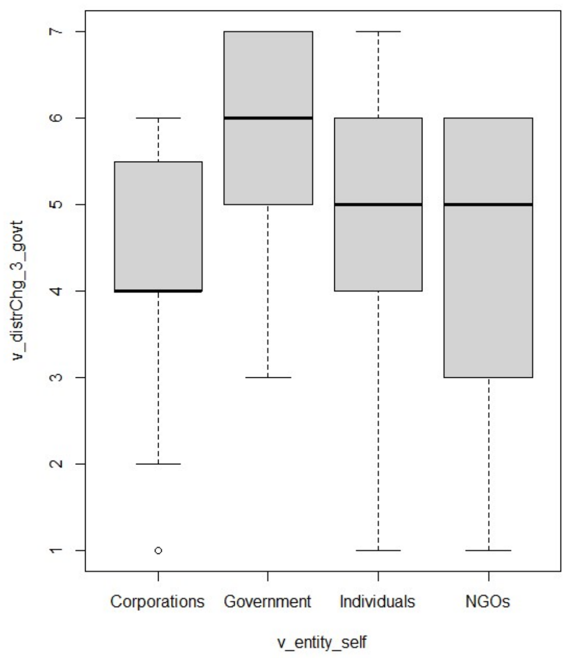

Figure 5.3. Boxplot, governments' decision right change

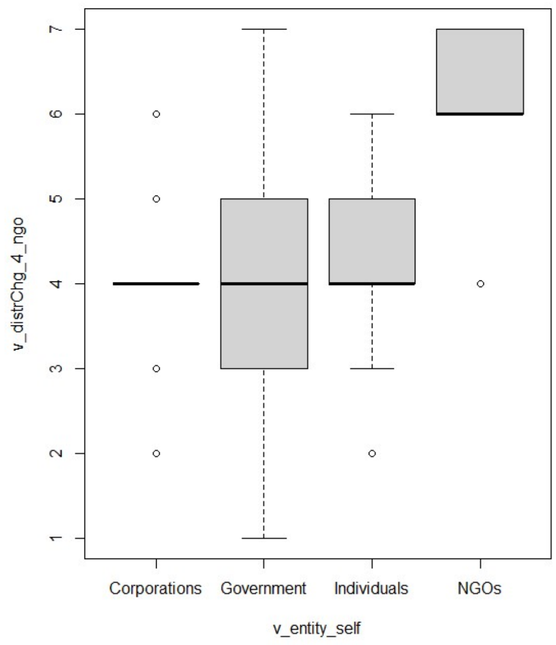

Figure 5.4. Boxplot, NGO decision right change

The means and boxplots above suggest differences among decision right changes when an entity is identified as the primary entity versus when it is not, as well as differences in decision right changes for the selected entity versus non-selected entities.

To confirm these trends, ANOVA was selected as it can test for significant differences across three or more different groups (Soetewey 2020). In this case, each ANOVA analysis tested the hypothesis that mean decision right changes for an entity was the same regardless of which entity was identified as the primary entity. If the p-value is 0.05 or less, then the hypothesis that all means are equal is rejected and there is confirmation that at least one group is different from the others.

Table 5.16 below shows the results for each of the four ANOVA analyses (each analysis looks at one entity's decision right change) generated by R's aov() function:

Table 5.16. H5 ANOVA results

Decision Rights Change for	*Df*	*Sum Sq*	*Mean Sq*	*F statistic*	*p-value*
Individuals	3	49.4	16.468	4.724	0.0040 **
Corporations	3	20.4	6.805	2.531	0.0615 .
Government	3	51.0	17.007	9.06	0.0001 ***
NGOs	3	20.5	6.842	4.367	0.0063 **

Based upon the p-values above, in three of the four analyses the null hypothesis that all means are equal are rejected, indicating that there are significant differences in decision right changes for governments, individuals, and NGOs when the various entities are identified as primary rights-gaining entities. The ANOVA for corporate decision right change was very close to the 0.05 level and warrants further examination along with the other entities to determine if specific pairings reveal differences.

Given the primary goal of comparing an entity's decision right change for cases where it was identified as the primary entity gaining rights compared to all other cases where other entities were selected, Dunnett's test was selected for post hoc analysis to derive additional insight as to which groups displayed differences based on the identified entity. Dunnett's test is particularly well suited to situations where multiple comparisons wish to be made against a reference group, which is exactly the case here (Soetewey 2020). For each entity, the decision right change is the measured variable and the comparison is when that entity is the identified primary entity compared to when each other entity is selected as primary. Dunnett's test was performed using the glht() function in the multcomp package of the R statistical programming language.

For the change in individual decision rights, Table 5.17 below shows the results for Dunnett's test:

Table 5.17. Dunnett's test for individuals' decision right changes across identified entities

Hypothesis to test	*Estimate*	*Std. Error*	*t value*	*Pr(>|t|)*
Corporations - Individuals == 0	-1.0735	0.5660	-1.8970	0.1616
Government - Individuals == 0	-1.3444	0.4185	-3.2120	0.0053 **
NGOs - Individuals == 0	0.7765	0.8943	0.8680	0.7473

From the table above, decision right changes for individuals differed significantly when respondents identified individuals as the primary beneficiary compared to cases where government was identified as the primary beneficiary, significant at the alpha = 0.01 level. This difference, combined with the lack of significant differences among the other groupings, suggests that the impact on individuals' decision rights is distinct in cases where individuals gain rights compared to when government gains rights. In cases where respondents identified corporations, individuals, or NGOs as the primary beneficiary, there were no significant differences in the effect on the decision rights of individuals.

Turning to change in corporate decision rights, the table below shows the impact across identified entities from the Dunnett test results:

Table 5.18. Dunnett's test for corporations' decision right changes across identified entities

Hypothesis to test	*Estimate*	*Std. Error*	*t value*	*Pr(>|t|)*
Individuals - Corporations == 0	-0.4779	0.4971	-0.9620	0.6398

Government - Corporations == 0	-1.1676	0.4745	-2.4600	0.0403 *
NGOs - Corporations == 0	-1.1250	0.8400	-1.3390	0.3915

Decision right changes for corporations differed significantly when the identified entity was government compared to corporations, significant at the alpha = 0.05 level. In cases where individuals or NGOs were identified entities, there were no significant differences in reported changes to corporate decision rights. Similar to the analysis of changes to individuals' decision rights, the only significant difference is between government and the entity whose decision right changes are analyzed.

The Dunnett's test results for changes to government decision rights are presented below:

Table 5.19. Dunnett's test for government decision right changes across identified entities

Hypothesis to test	*Estimate*	*Std. Error*	*t value*	*Pr(>|t|)*
Corporations - Government == 0	-1.7083	0.3955	-4.319	< 0.001 ***
Individuals - Government == 0	-1.1311	0.3071	-3.683	0.0011 **
NGOs - Government == 0	-1.6958	0.6438	-2.634	0.0285 *

In the case of government decision rights, there were significant differences between government and each of the other entities when identified as the primary entity. The differences between corporations and government were most significant (at alpha = 0.001), followed by individual and government differences (significant at alpha = 0.01), and finally NGOs and governments (significant at alpha = 0.05). This confirms results from the prior Dunnett's test analyses where only governments were found to differ significantly in the cases of corporate and individual decision rights; it is apparent that the differences between cases where government is the beneficiary are different from all other cases and government decision rights is distinct from the other groups.

The final case to analyze is the decision right changes for NGOs when NGO was the primary entity compared to cases when it was not. Dunnett's test results for this case is shown below:

Table 5.20. Dunnett's test for NGO decision right changes across identified entities

Hypothesis to test	*Estimate*	*Std. Error*	*t value*	*Pr(>|t|)*
Government - NGOs == 0	-2.0909	0.5907	-3.5400	0.0015 **
Corporations - NGOs == 0	-1.8750	0.6413	-2.9240	0.0092 **
Individuals - NGOs == 0	-1.6765	0.5995	-2.7960	0.0133 *

From the table above, NGO decision right changes differed significantly in each pairing indicating distinct differences in NGO decision right changes in cases where NGOs are the primary entity compared to each of the cases when it was not. The differences were greatest in the NGO-Government and NGO-Corporation pairings, significant at the alpha = 0.01 level, and significant at the alpha = 0.05 level when NGOs and Individuals were compared.

Analysis of H5 indicates that decision right changes differed significantly when an entity was selected as the primary entity compared to when it wasn't, demonstrating a relationship between the entity selected and its change in decision rights. Further analysis comparing the groups in each case indicated that the most distinct differences are between government and other entities, with no significant differences found between a number of pairings such as changes to individual decision rights when comparing individuals and corporations. Thus, H5 is confirmed.

H6: An individual's desire for privacy, anonymity, and expected behavioral responses will be affected by the type of entity (group) that gains decision rights

Analysis of H6 and H7 relied on statistical calculations from the R package SEMinR, following procedures outlined in Hair et al 2021 regarding conducting PLS-SEM analysis in R.

The first step in analyzing H6 was to create a series of four dummy (flag) variables indicating when the self-identified entity was individuals, corporations, government, and NGOs (1 when the condition was true, 0 when not). Following best practices for use of categorical data to comprise a composite PLS-SEM construct, the data was standardized to eliminate perfect correlation between variables and to ensure zero-mean data (Hair et al 2019). The dummy variables were standardized following Lohmoller's formula outlined in section (v) of Table 4.4 (Lohmoller 1989, pg. 159). Correlations of the standardized variables are shown below:

Table 5.21. Correlations between standardized dummy variables

	ent_self_ind_nc	*ent_self_corp_nc*	*ent_self_govt_nc*	*ent_self_ngo_nc*
ent_self_ind_nc	1	-0.29341	-0.64731	-0.17036
ent_self_corp_nc	-0.29341	1	-0.39661	-0.10438
ent_self_govt_nc	-0.64731	-0.39661	1	-0.23028
ent_self_ngo_nc	-0.17036	-0.10438	-0.23028	1

None of the standardized variables appear to exhibit over-correlation with each other, with the closest being -0.64 (-1.0 would be perfect negative correlation).

H6 makes use of the ENTITY, IPC, REG, SOC, and BI constructs. The results from H1 and H2 indicated respondent difficulty in identifying the entity that gains rights as designed by the researcher. Due to this difficulty, self-identified entity is used for all subsequent analyses as it represents an individual's frame of mind and the perspective from which they are approaching decision right changes. Using the researcher designed entity, or using each of the four vignettes as a basis for organization of the analyses, would be confounded by what respondents perceive and would involve evaluating responses relative to an entity that they do not believe they are responding to.

In evaluating the potential effect of ENTITY on BI (behavioral intentions), the constructs IPC, REG and SOC were included in the model as moderator variables, hypothesized to impact the relationship between ENTITY and BI. Moderation is defined as "…a situation in which the relationship between two constructs is not constant but depends on the values of a third variable, referred to as a moderator variable." (Hair et al 2021, pg. 156). This is exactly the hypothesized situation, and therefore the use of these variables as moderator variables is justified. There are multiple methods of calculating moderating effects, the latest recommendation is to use a two-stage approach where stage 1 consists of the main effect model without any interaction terms (and moderator variables affecting the outcome variable) and stage 2 involves utilizing stage 1 results to create an item used to measure the interaction term (Hair et al 2021). This approach takes advantage of the natural strengths of PLS-SEM methods to calculate latent variable scores (Hair et al 2021). In the SEMinR package, the entire model is specified in one step, with two-stage selected as an option. Thus, the measurement model includes both the moderator variables with direct relationships to the outcome variable as well as interaction terms consisting of the moderator variables and the variable whose effect is being tested on the outcome variable.

All constructs used in the model are reflective, and the standard evaluation criteria used to evaluate reliability and validity are used (Hair et al 2021, chapters 4 and 5):

1. Indicator level reliability: indicator reliability (indicator loadings)
2. Construct level reliability: internal consistency reliability (Cronbach's alpha)
3. Convergent validity: average variance extracted (AVE)
4. Discriminant validity: heterotrait-monotrait ratio of correlations (HTMT)

Indicator reliability evaluates the extent to which the construct items load on the construct (or represent the construct). In evaluating indicator reliability, indicator loadings of 0.70 or above are recommended, although loadings can be considered all the way down to 0.40. Another method is to square the loadings and evaluate those values against a desired threshold value of 0.50 (Hair et al 2021). Below are the squared indicator loadings:

Table 5.22. Squared indicator loadings, H6

Item	*IPC*	*REG*	*SOC*
privconc_overall	0.827	0	0
pc1_Mas_v1	0.721	0	0
pc2_Mas_v2	0.625	0	0
c3_Mas_v3	0.774	0	0
pc4_Mas_v4	0.597	0	0
pc5_Mas_v5	0.511	0	0
pc6	0.635	0	0
pc_7	0.594	0	0
pc_8	0.630	0	0
cocit_reg1	0	0.731	0
cocit_reg3	0	0.886	0
cocit_reg4	0	0.916	0
cocit_reg5	0	0.209	0
cocit_soc1	0	0	0.840
cocit_soc3	0	0	0.747

Note that BI is not shown as it is a single-item construct and has a loading by definition of 1.0, interaction terms are not shown as they are not evaluated using this method, and the ENTITY construct items are a composite categorical construct and not assessed on indicator reliability due to their nature (see previous discussion regarding the standardization of these variables). From the above table, all of the squared loadings are above the desired threshold of 0.50 except for the item cocit_reg5 at 0.209. Given the strength of the other REG construct items, cocit_reg5 was removed from the model with the revised results for the REG construct shown below:

Table 5.23. Squared indicator loadings, REG construct (revised)

Item	*REG (revised)*	*REG (Orig. Est.)*
cocit_reg1	0.769	0.731
cocit_reg3	0.875	0.886
cocit_reg4	0.916	0.916
cocit_reg5	Not included	0.209

All of the remaining items load highly on the REG construct and are kept for model estimation.

The internal consistency reliability of the constructs was measured using Cronbach's Alpha, with a desired alpha of 0.70 or higher indicating the items within the construct are more or less homogenous. Table 5.24 below shows the results of the reliability calculations (including Cronbach's alpha) produced by the SEMinR package:

Table 5.24. Reliability measures, H6

	alpha	*rhoC*	*AVE*	*rhoA*
IPC	0.944	0.945	0.657	0.832
REG	0.913	0.946	0.853	0.934
SOC	0.743	0.885	0.793	0.769

The alphas are all above 0.70, with two of the constructs having alphas of above 0.90 indicating superior internal consistency reliability.

Next the validity of the model is assessed. Convergent validity measures how well the construct hangs together and explains the variance of its respective items. The average variance extracted is a measure of the communality of a given construct and is used here to assess the convergent validity with a desired AVE for a construct of 0.50 or above; an AVE of 0.50 or higher indicates that the latent construct explains at least 50% of the variance of the items that make up the construct (Hair et al 2022). The table above indicates that the AVE for the three reflective constructs ranges from 0.657 (IPC) to as high 0.853 (REG), above the minimum threshold of 0.50.

Discriminant validity is the extent to which a construct is distinct from the other constructs used in the model, as constructs purported to measure different latent variables should have items that are distinct from each other and not highly correlated. To assess Discriminant validity the heterotrait-monotrait ratio of correlations (HTMT) was utilized as it provides an excellent measure of discriminant validity (Hair et al 2021). The threshold value for the HTMT used was 0.85, meaning that value between constructs should be as low as possible, but not higher than 0.85 (Henseler et al., 2015). Table 5.25 shows the HTMT calculations produced by the SEMinR package:

Table 5.25. HTMT criterion, H6

	IPC	*REG*	*SOC*
IPC	.	.	.
REG	0.170	.	.
SOC	0.183	0.234	.

The HTMT values above are all well below 0.85 and are indicative of constructs that have items that load onto their own construct and not onto another construct highly.

With the reliability and validity of the model assessed, the next step is to assess the model itself. As outlined by Hair et al in their 2021 book covering PLS-SEM modeling in R, bootstrapping the model and then inspecting the structural paths of the bootstrapped model is one effective method of evaluating the strength and predictive value of a model. The table below shows the bootstrapped (and original) path estimates:

Table 5.26. Bootstrapped PLS-SEM path estimates, H6

	Original Est.	*Bootstrap Mean*	*Bootstrap SD*	*T Stat.*	*2.5% CI*	*97.5%CI*	*CI excludes zero*
ENTITY -> BI	0.073	0.121	0.128	0.573	-0.182	0.322	
IPC -> BI	0.132	0.134	0.158	0.835	-0.307	0.360	
REG -> BI	-0.387	-0.381	0.091	-4.243	-0.556	-0.187	X
SOC -> BI	-0.097	-0.097	0.103	-0.945	-0.284	0.118	
ENTITY*IPC -> BI	0.137	0.063	0.153	0.895	-0.215	0.355	
ENTITY*REG -> BI	-0.006	0.002	0.156	-0.037	-0.274	0.317	
ENTITY*SOC -> BI	0.061	0.027	0.164	0.369	-0.249	0.274	

Figure 5.5 below shows the entire bootstrapped measurement model:

Bootstrapped Model - H6

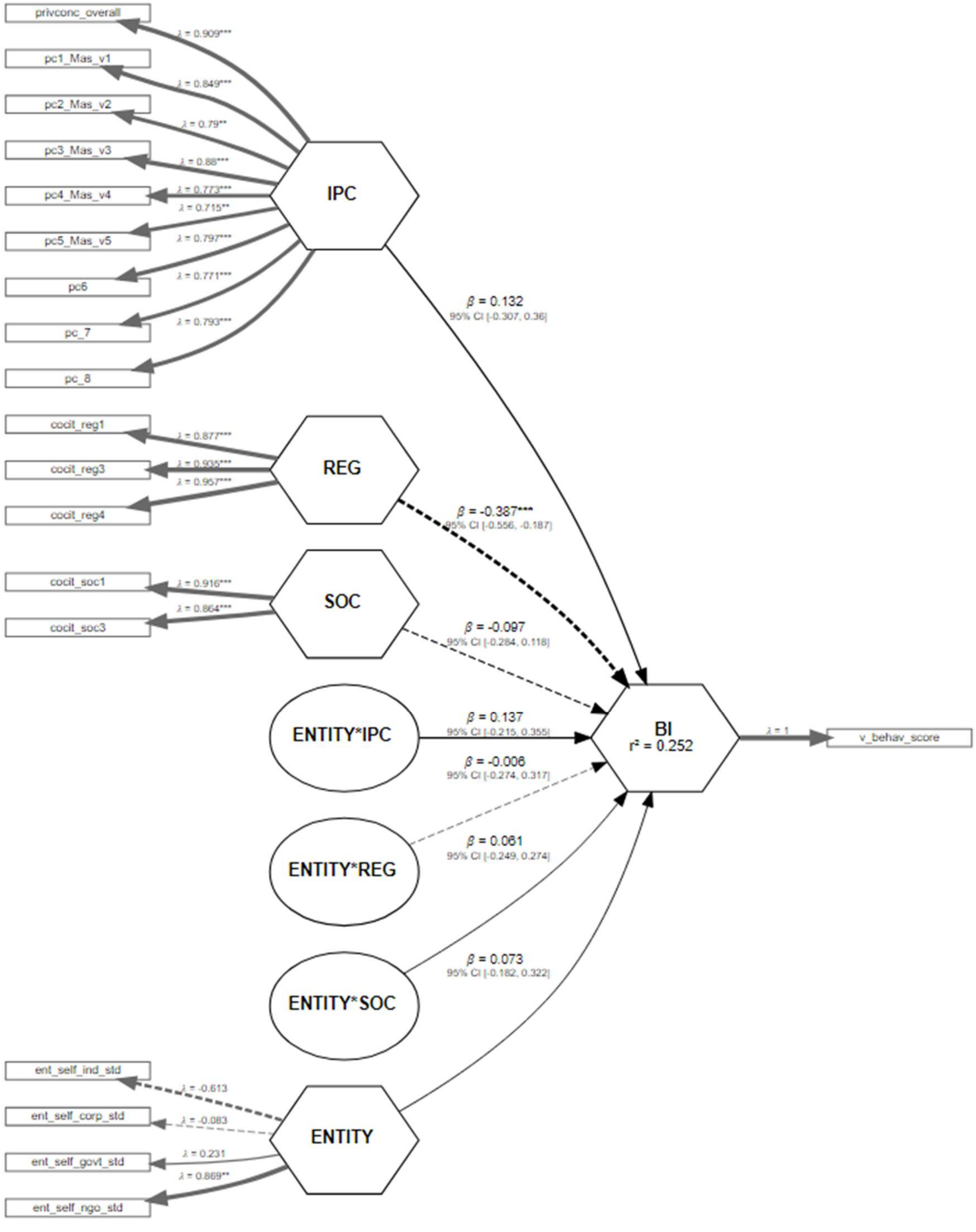

Figure 5.5. H6 Bootstrapped PLS-SEM Measurement Model

Based on the bootstrapped model estimates, the only relationship that was statistically meaningful was that between REG and BI, as the 95% confidence interval does not include zero and is therefore significant (Hair et al 2021). Therefore, regulatory environment is the only hypothesized construct with any significant effect on the outcome variable (BI) and because the self-identified entity did not have a significant effect on BI hypothesis H6 is not confirmed.

H7: Changes to decision rights will directly affect outcomes

H7 adds the decision rights change (DRChg) construct to the model estimated in H6. The DRChg construct used a measure of absolute change across all the entities, summing the absolute change of each for a single value to represent the level of change induced by the scenario. The structural model therefore differed from the one in H6 in two ways: first, the DRChg construct is added as a predictor of BI and as a moderator of the ENTITY -> BI relationship; second, the interaction effects of REG, SOC, and IPC were removed and these constructs were used simply as predictors of BI. The latter change was done due to (a) the low number of survey responses where simply adding a new construct pointing to the dependent variable would risk having too many constructs pointing at a single outcome when keeping all of the additional interaction terms, and (b) due to the results of H6 indicating that the interaction terms did not have an effect on BI while the direct relationship of REG -> BI was significant.

As with H6, the reliability and validity were assessed using squared item loadings for internal consistency, Cronbach's alpha for internal consistency reliability, AVE for convergent validity, and HTMT for discriminant validity. The same threshold criteria were used from Hair et al 2021 as in H6, and these criteria need to be re-evaluated here as the changes to the measurement model from H6 will affect the calculated values and characteristics of the model.

Results for the squared loadings are presented below:

Table 5.27. Squared item loadings, H7

	IPC	*REG*	*SOC*
privconc_overall	0.827	0	0
pc1_Mas_v1	0.721	0	0
pc2_Mas_v2	0.625	0	0
pc3_Mas_v3	0.774	0	0
pc4_Mas_v4	0.597	0	0
pc5_Mas_v5	0.511	0	0
pc6	0.635	0	0
pc_7	0.594	0	0
pc_8	0.630	0	0
cocit_reg1	0	0.769	0
cocit_reg3	0	0.875	0
cocit_reg4	0	0.916	0
cocit_soc1	0	0	0.840
cocit_soc3	0	0	0.747

All items have a squared loading above 0.50, and thus are internally consistent across their respective constructs. Reliability measures for the model are shown below:

Table 5.28. Reliability and validity statistics, H7

	alpha	*rhoC*	*AVE*	*rhoA*
IPC	0.944	0.945	0.657	0.832
REG	0.913	0.946	0.853	0.934
SOC	0.743	0.885	0.793	0.769

Note that DRChg, BI, and ENTITY are not shown above. DRChg and BI are single-item constructs and have values of 1.0 for all the above listed criteria, and ENTITY is a composite categorical item that is not expected to possess any type of internal consistency or reliability as they are not measuring the same concept but rather are standardized dummy variables with mean equal to 0.

The table above indicates that the Cronbach's alpha for each of the listed constructs is above the threshold value of 0.70, and therefore the items are internally consistent. Additionally, the AVE values are all above the cutoff value of 0.50, and all constructs exhibit convergent validity.

Finally, the discriminant validity is assessed using the HTMT values:

Table 5.29. HTMT results, H7

	IPC	*REG*	*SOC*
IPC	.	.	.
REG	0.17	.	.
SOC	0.183	0.234	.

There do not appear to be high correlations between any of the distinct constructs, with the highest reported HTMT value being 0.234 (well below the 0.85 cutoff value).

The R-squared values and path estimates for the model are shown below:

Table 5.30. PLS-SEM Path estimates, H7

	DRChg	*BI*
R^2	0.039	0.231
AdjR^2	0.030	0.192
ENTITY	0.197	0.089
DRChg	.	-0.032
IPC	.	0.131
REG	.	-0.401
SOC	.	-0.111

The relationship between ENTITY and DRChg has a path estimate of 0.197, not particularly large. The other main path of interest to H7, that between DRChg and BI, was -0.032. None of the paths were significant and given the limited relationship between DRChg and BI evidenced by the path estimate, H7 is not confirmed. The measurement model for H7 is presented in Figure 5.6 below:

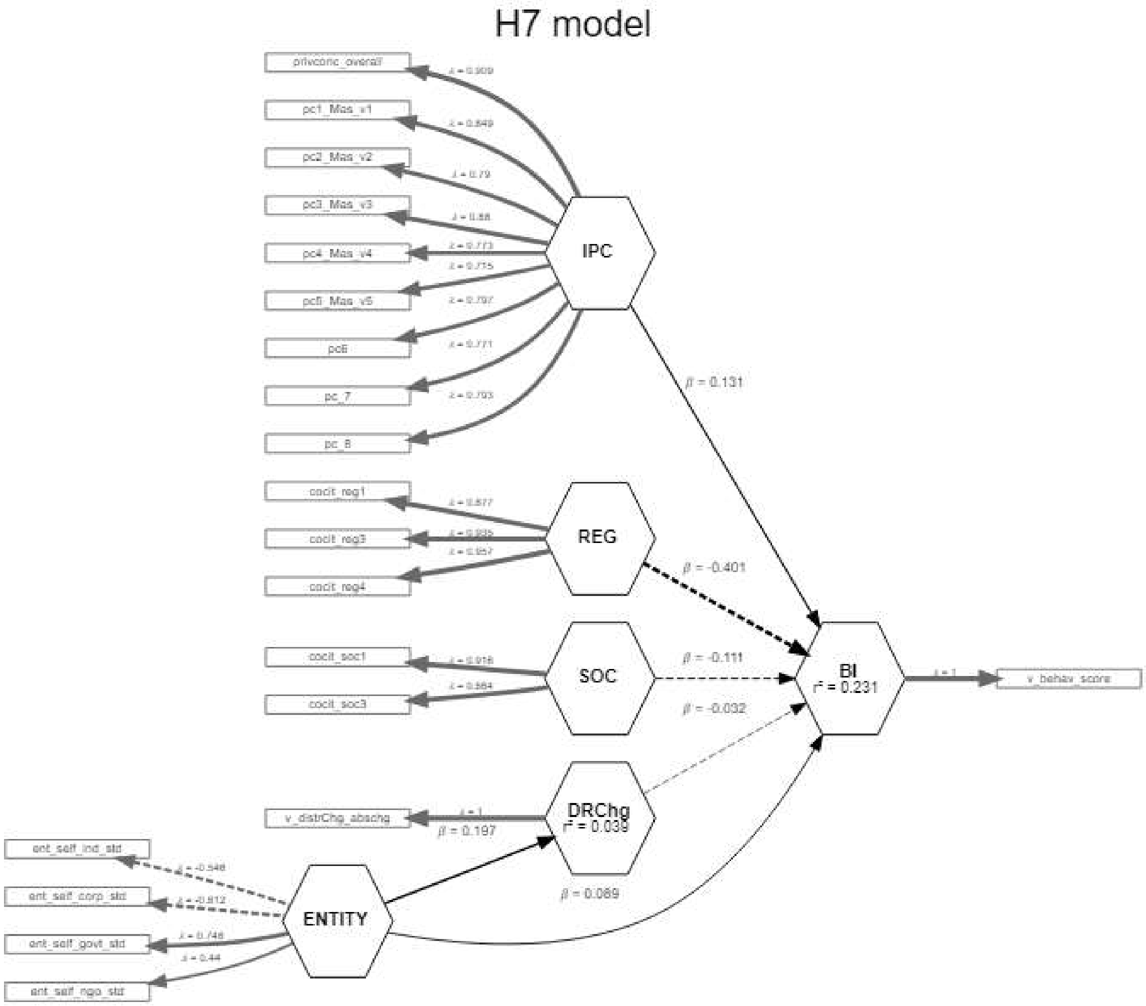

Figure 5.6. Measurement model, H7

Overall Summary of Hypotheses

A summary of the hypotheses and their results are shown in the table below:

Table 5.31. Summary of Hypotheses

H	*Hypothesis*	*Result*

H1	Societal attitudes and regulatory environment will have a significant impact on an individual's initial threat perception	Not confirmed
H2	Societal attitudes, regulatory environment, and the distribution of information decision rights will have a direct effect on an individual's threat perception	Partial suggested but not confirmed: suggested effect of DoR on PThr
H3	Individuals will correctly identify who benefits (gains decision rights) in each vignette	Partial confirmation: confirmed for government, not for corporations or individuals
H4	The entity (group) assigned the primary decision rights in each vignette will see an increase in their share of decision rights	Confirmed
H5	Entities (groups) not assigned the primary decision rights will see either no change or a decrease in decision rights	Confirmed
H6	An individual's desire for privacy, anonymity, and expected behavioral responses will be affected by the type of entity (group) that gains decision rights	Not confirmed
H7	Changes to decision rights will directly affect outcomes.	Not confirmed

Chapter 6: Conclusion

Discussion

Digital information privacy is an oft researched topic, and yet it remains a stubbornly amorphous concept. The topic has gained traction across disciplines with a number of contextual interpretations present in Information Sciences, Law, Economics, Psychology and Anthropology among others.

Within Information Sciences, privacy and privacy concern constructs have been well established utilizing the APCO model that deals with antecedents, information privacy concerns themselves, and the outcomes of such concern. The current research attempts to bring together the disparate conceptualizations of the subject and revisit the underlying structure of the ubiquitous APCO model in an effort to allow researchers to conduct relevant research in advance of technical development and deployment, seeking to accomplish the following four goals: (1) expand privacy research into more future-relevant modes of theorizing via more speculative and dialog-based theorizing, (2) integrate IS privacy ideas with those present in other fields in an effort to unify notions of privacy, (3) utilize ideas from goals 1 and 2 to develop a new framework through which to approach privacy research that better accounts for social structures, and (4) utilize the framework to assess the impact of theoretical changes to existing distributions of information decision rights across various countries.

Framework development drew from the most dominant modes of privacy research withing IS as well as coverage across other fields, and included privacy-adjacent ideas that are often not discussed such as anonymity in an effort to obtain wider coverage and relevance. The conceptualization drew on foundational IS research that demonstrates privacy is a multi-level concept, re-configured the levels (individual, group, organizational, societal) into their most recognizable instantiations (individuals, government, corporations, society) and introduced the concept of 'decision rights', meaning that in order for any real choice to be made regarding privacy the actor must also possess the agency to do so. These decision rights (whether explicitly assigned or not) are bounded in that new technologies do not inherently expand the overall decision right space, but merely affect the distribution of such rights across actors within a society. This allows the levels to be thought of as actors that can impact the actions of the other actors, and there is an idea of equilibrium introduced to describe the existing interplay amongst the actors (entities). This allows for actions of any actor(s), instantiations, and constructs to be evaluated in terms of both their impact within any given actor (level) as well as the impact on the existing equilibrium (distribution of decision rights). The cycle of technology -> concern -> awareness -> adaptation is unending, and the proposed framework considers the actor (individual, corporation, government), the relevant threat vector(s), and potential sources of resolution (who has agency to implement) in an effort to find a socially acceptable balance/equilibrium prior to a technology's development and/or implementation.

The framework was then operationalized, combining enhanced APCO constructs with newly developed constructs, focusing on the following areas: the nature of perceived threats, the viability of forward-looking vignettes as a research tool, the impact of various changes to decision rights on behavioral intentions, and the role that changes to decision rights equilibria play in planned behavioral responses. To explore these areas, the following research questions were developed:

- RQ1: How do individual privacy concerns, regulatory environment, and societal values affect an individual's threat perception? (H1 and H2)
- RQ2: How predictable are the changes to decision rights based on the vignettes? (H3 – H5)
- RQ3: How do the various decision rights scenarios (vignettes) affect outcomes? (H6)
- RQ4: How do changes in decision rights as a result of the vignettes affect outcomes? (H7)

In exploring RQ1, neither societal attitudes nor regulatory environment had a direct impact on an individual's overall threat perception. However, the distribution of rights did have noted impacts on threat perception, particularly the type of distribution regime as opposed to any individual configuration of dominant entity. The type of regime, or the degree of concentration, had an impact on perceived threat levels, and the degree to which individuals in society possessed a base level of decision rights also affected threat perception.

With regards to RQ2, changes that impacted government decision rights were relatively easy to detect, and these scenarios were well differentiated from scenarios that involved any of the other entities. At times entities such as individuals and corporation moved together in response to a scenario, government tended to move in the opposite direction in terms of rights changes than all the other entities (groups). Additionally, vignettes that involved changes to corporate or individual decision rights were difficult for respondents to identify, indicating a more intertwined nature of individual and corporate spheres of control when it comes to new technologies. To illustrate, in a situation where an app did something perceived as beneficial, respondents often indicated that their decision rights would increase even though all data would be collected, controlled, and governed by the purveyor of the technology, thereby granting the organization access to information in an area of individuals lives they previously did not have access to. Given the difficulty in respondents' ability to identify the primary entity gaining decision rights, analyses were based on the reference point of which entity the respondent identified as the primary entity gaining decision rights as opposed to which vignette the response belonged to. In all cases, the identified entity saw an increase in their share of rights that was distinct from changes when the entity was not selected. Amongst the groups, differences in mean decision right changes was highest among government and lowest among corporations. In looking at each pairing of groups for when an entity was selected as the primary beneficiary: individuals and governments were distinct (the first entity listed was the reference group), corporations and government were distinct, government was distinct from all other entities, and NGOs were distinct from all other entities. Combined with the results related to RQ1, there is a duality that emerged in terms of the inability to assess, outside of government, which entity was gaining rights in the vignettes while showing clear and consistent patterns of right changes for perceived entities.

With regard to RQ3, or the impact of the vignettes on outcomes, the only significant relationship was between the strength of the regulatory environment and an individual's behavioral intentions (the actions they reported they would take in response to a given situation).

The addition of decision rights changes to the model (RQ4) did not yield any additional insight beyond those found in RQ3 (H6), as there was no observed impact of the change in decision rights on behavioral intentions. This speaks to the difficulty in conceptualizing and measuring decision rights changes; given that respondents had difficulty in identifying the entity that stood to gain rights it is not surprising that it was difficult to disentangle the actions they would take as a result of changes to those rights. The level of abstraction used likely needs to be lowered and explored further in order to be an effective construct.

In looking at broader demographic trends, there were some interesting results. While US citizenship did not really affect reported mean privacy concern levels, there were differences across geographic regions. In descending order, from most concerned to least concerned the results were: Africa, Asia, North America, Middle East, South America, Europe. In addition, the difference between Europe and the other regions was stark: Europe was the only region to report a mean privacy concern less than 4.0 (reported mean was 2.67) on a 7-point scale. Combined with the observed impact of regulatory environment on perceived threat level, this indicates that the regulatory environment as a concept is important when researching privacy concerns and threat perception. Europe has the strictest privacy laws (in terms of providing more protections to individuals) of any of the regions and it is hardly surprising to observe this result, but the degree of difference is noticeably large. Another demographic difference that may be of interest was that male respondents reported higher levels of privacy concern than female respondents.

Beyond the analyses related to the hypotheses, there were interesting trends observed in the reported changes to decision rights as a result of the vignettes; each vignette will be discussed briefly below to provide necessary context and findings of interest.

The first vignette was designed to transfer decision rights to the government (largely at the expense of individuals), describing a situation where the government contracts with a corporation to utilize their artificial intelligence systems, connecting it to existing cameras installed in public spaces for use in law enforcement efforts. The mean decision right changes reflected the expansion of government rights, with government having the largest rights increase (mean decision right change of 5.7 on a 7-point scale, where 4.0 = no change, values less than 4.0 represent a decrease in rights, and values greater than 4.0 represent an increase in rights). Corporations also saw a slight increase in decision rights (mean of 4.5), while individuals and NGOs reported an overall decrease in decision rights (3.26 and 3.88, respectively). Given the construction of the scenario, it is not surprising that corporations saw an increase in decision rights along with governments, as the underlying technology deployed was theirs. The results in this scenario were clear cut and relatively straightforward to assess by respondents.

The second vignette was designed to increase the share of decision rights afforded to corporations, describing a situation where a new technology is marketed towards use by individuals but where corporations are increasing their reach and control of this information. Specifically, the scenario describes a flexible patch that provides real-time data on an individual's organ function and blood chemistry that will come with an app that can connect to the sensors in an effort to "reconstruct images of soft tissue, analyze blood chemistry, and provide personalized recommendations." The scenario specifically mentions upstream use of the data collected by the sensors in an effort to highlight the corporate rather than individual control, despite the marketing of the technology towards the end user. Respondents reported the largest decision right increase in this scenario for individuals, not corporations. All entities reported an increase in decision rights in this scenario, with individuals reporting the largest gain. Individuals had a mean decision right change of 5.04 (4.0 is no change), corporations had a reported mean value of 4.74, the government mean was 4.41, and the NGO mean decision right change was 4.26. Despite key pieces of information in the scenario pointing to the lack of individual control, respondents felt this gave the largest decision right benefits to individuals. While the technology would undoubtedly stand to benefit individuals in ways unrelated to privacy and decision rights, it does not expand their decision rights in any real way as presented; this apparent conflation of benefit and decision rights was observed previously and necessitated performing analyses based on self-identified entity as opposed to researcher-identified entity (to evaluate the hypotheses and model effects), and primarily impacted scenarios and entities other than governments. It is clear that future endeavors in this area should seek to understand and mitigate this effect.

The third vignette was designed to transfer decision rights to individuals, describing a scenario whereby corporate charters are amended such that their responsibilities to shareholders go beyond fiduciary to include responsible data management. The scenario outlines that corporations can now be held liable for mismanagement or negligence concerning data and outlines a number of limits placed on corporate data collection. As with vignette #2, all entities saw an increase in decision rights as a result of the changes. Government saw the largest increase in decision rights (mean = 4.92), with corporations seeing the second-largest increase (mean = 4.77). NGOs reported a mean decision right change of 4.42 and individuals at 4.35. The fact that corporations reported an increase despite the restrictions placed on them in the scenario description is quite interesting, and again supports the decision taken to analyze the hypotheses with respect to the self-identified entity as opposed to by vignette (if entity identification were more accurate, perhaps by-vignette analysis could have been feasible).

The fourth and final vignette was designed to expand government decision rights, describing a scenario by which the government requires metadata appended to all internet traffic of their specification along with their tapping into existing internet cables entering and exiting the country to collect and archive data with a purported purpose of cracking down on corporate espionage. Government did indeed see the largest decision right increase, with a mean decision right change of 5.77 (4.0 = no change, greater than 4.0 is an increase and less than 4.0 is a decrease in rights), with NGOs also seeing an increase in rights (mean = 4.42). Corporations and individuals reported decreases in decision rights (corporate mean = 3.77, individual mean = 3.85).

Implications

Research

The research presented has several implications for privacy research. With regards to established IS privacy research, the use of several APCO constructs (a) confirmed that regulation has an effect on privacy and privacy-related behaviors, and (b) where regulation has been previously demonstrated to have significance as an antecedent to privacy it has now been suggested to have a direct effect on behavioral intentions. This suggests that the larger approach to privacy afforded by conceptualizing multiple actors as having agency is worth developing and exploring in future strands of research.

Additionally, each of the two main components of the research have implications for research. Those two primary components were (1) the development of a framework through which to explore how the various societal actors impact privacy, and (2) operationalization and testing of that framework.

Development of the framework contributes to research by melding conceptualizations of privacy across fields for use in future research and by providing a potential foundation for additional different operationalization choices. Such choices might include analysis of interactions among groups and/or changes in decision right equilibrium to better understand dynamics among groups, or exploration of perceived threats by group.

The operationalization of the framework utilized here contributes to research broadly in the pursuit of new avenues of speculative research that are future-oriented via the use of vignettes, and more specifically in illuminating in a different manner the multi-level nature of privacy: government decision rights are easily understood and the impact of government rights and other entity rights are clearly delineated, while impacts surrounding changes in rights of the other groups are less so. More work could be done here to shed light on these differences, perhaps by diverging further from solely empirical methods and including qualitative explorations of these ideas.

Finally, the research served as an initial foray into the use of vignettes to explore the information privacy space. The vignettes demonstrated a striking amount of variability with respect to the actors involved and the impact on decision rights to the respective groups, suggesting that responses vary widely depending on the specific within each scenario. Further, it makes clear the need for carefully crafted vignettes that would ideally be combined with more in-depth data collection and analysis methods such as qualitative methods to support the vignettes.

Practice

The implications for practice include information regarding different geographic approaches and the development of regulations and norms surrounding information privacy. The regional differences in levels of concern and perceived threat indicate that the social negotiation of norms and rights will need to look different. It is of great importance now to consider the distribution of rights and how societies envision themselves developing, including what guardrails are deemed necessary prior to potential changes, and the framework presented here can aid in thinking about crafting regulations and how to balance the needs of various constituents across a society. Countries are increasingly grappling with issues related to information privacy, attempting to catch up with pace of past technological changes. This pre-norming approach where impacts are considered in advance of potentially disruptive changes is being increasingly exhorted with regards to particularly sensitive and potentially dangerous technologies such as AI and biological modification technologies, and information privacy should be no different.

The findings yield a few suggestions for regulators: you cannot rely on individuals to accurately determine when their privacy is at risk – responses to the vignettes indicate a conflation of benefit with decision right, and a degree of entanglement among corporate and individual rights such that it is difficult for individuals to assess potential impacts. This also suggests that corporations, at least in current environment, will likely be able to placate concerned consumers with vague assurances of privacy and window-dressing methods of protection; the more beneficial the technology to the individual and more empowered they feel in use they will likely conflate that with security of their information.

Limitations

The primary limitations stem from the operationalization of the framework and the choice of survey instrument. The decision to make use of vignettes places extra importance on the wording of the vignettes, as respondents need to understand clearly what is being asked. In this way, the vignettes introduced an additional measure of researcher variance, as a scenario with a number of specific details is more subjective than a typical survey question (which while still subjective is typically shorter and more direct). Additionally, the difficulty and complexity of some of the ideas introduced surrounding privacy applies to perhaps a greater extent to ideas surrounding the distribution of decision rights. And indeed, respondents did have some difficulty in assessing who would gain rights. Decision rights as a concept needs to be examined for alternate methods of capturing this information.

While the study explored groups and agents beyond individuals to a great er extent than prior research, the survey as constructed still represents at its heart an individual-centric model in terms of measuring external constructs such as regulatory environment (filtered through individual perception) and decision rights. More concrete and external measures of these constructs would be ideal, along with careful vetting and crafting of vignettes that isolate only the desired change.

The above limitations combined with the relatively low number of responses suggest against any forceful conclusions. Different analysis methods beyond quantitative analyses, such as qualitative methods such as focus groups are recommended to explore these ideas further and attempt to make further sense the results.

Conclusion

IS research has a well established thread of privacy research that has yet to penetrate the broader societal discussions taking place regarding the issue. The current research reviewed prior IS work, surveyed work across other fields, and included related topics that have been under-studied in an effort to bring much of this work together in a framework that can be used to assess the impact of technologies and changes prior to their implementation. The framework was then operationalized using a model based on established IS privacy constructs integrated with new larger constructs that represent the larger societal forces at play with respect to information privacy. The research demonstrated the use of vignettes in privacy-related research and explored the distribution of information decision rights across societal actors, contributing to future privacy research while providing practical recommendations for regulators.

Appendix A: Survey Instrument

Welcome! Thank you for your interest in participating in this research project, a brief overview can be found below, followed by the informed consent form on the following page.

Purpose.
The purpose of this research is to explore the relationship between individual ideas surrounding privacy and anonymity, societal structures and attitudes on these topics across countries, and future privacy responses. Each country has its own distribution of digital information rights; whether it be individuals, corporations, governments, or some mixture of them all that decide how digital information that relates to individuals is used, we want to explore how changes in that relative distribution affects those living in that society.

How your response will be used.
Information you provide will only be analyzed and presented in the aggregate. Additionally, the survey will collect anonymized responses meaning that no potentially identifying information (such as IP address, browser, etc.) will be linked to your response data in qualtrics. The only potentially identifying piece of information requested is your email address, but that is ONLY requested if you indicate you are interested in participating in an online focus group at the end of the survey, as we need a way to get in contact with you (if you are not interested in this, the survey asks for no information that could identify you).

Survey Completion.
While it is possible to complete the survey on a mobile device, we highly recommend the use of a computer to have the best possible experience with the survey. Some of the text and explanations may appear illegible on a mobile device.

Citizenship.

Part of this research project looks at differences among countries, and therefore we ask for citizenship information. While providing information regarding citizenship is beneficial to the project, it is in no way required.

Are you a US citizen?

○ Yes

○ No

Do you also have citizenship in a country other than the US?

○ Yes

○ No

Which non-US country are you a citizen of?
If you are currently (or have been) a citizen of more than one non-US country, please **provide the one**

country you identify most with (future sections of the survey will refer to the country you enter in the box below).

____

How many years have you spent in your original/primary country of citizenship? (please enter the nearest whole number)

____

The remainder of the survey is broken into 5 main sections. You can expect the survey to take between 15 and 30 minutes to complete, and the following is provided to give you an idea of what to expect:

- Privacy (5 minutes)
- Privacy and Anonymity (2 minutes)
- Regulatory Environment (2 minutes)
- Societal Attitudes (6 minutes)
- Vignettes (10-15 minutes; 4 future scenarios w/questions)

Section 1: Privacy.

Privacy is a term that can encompass a large number of related ideas, depending on its context. It has been expressed as a state (being in a state of privacy or not), a right, or an economic good.

This survey is interested in the idea of privacy as an exercise of individual choice (the choice to either share or keep secret) regarding information about oneself and its potential future uses. The idea of potential future uses means that privacy has a forward-looking aspect, as the collection and storage of information can have an impact on the future choices available to an individual (for example what loans an individual may receive). Focusing on the exercise of choice also confers some form of decision rights to individuals in order to be able to make those decisions.

Following is the formal definition used in the current study, please use it to contextualize and inform your responses as you see the term privacy appear in the survey:

'control over information that regulates access to the self in order to enhance current and future decision and behavioral choice'
References: (Zuboff 2015, p. 83), (Margulis 2003, p. 415)

The following section asks about your personal feelings and opinions surrounding the idea of privacy.

privconc_overall Overall, how concerned are you about the privacy of information that pertains to you that has been collected and stored digitally?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc1_Mas_v1 How concerned are you about websites/apps/devices collecting and using information about your activity?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc2_Mas_v2 How concerned are you about websites, apps, and devices recording and sharing your data with unknown third parties?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc3_Mas_v3 How concerned are you about websites, apps, and devices tracking your behavior?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc6 How concerned are you about websites, apps, and devices identifying you based on your online activity?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc4_Mas_v4 How concerned are you about institutions, public agencies, or intelligence services monitoring your online activity?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc5_Mas_v5 How concerned are you about not having insight into what institutions, public agencies, or intelligence services do with your data?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc_7 How concerned are you about institutions, public agencies, or intelligence services collecting and analyzing data gathered from website and app providers?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc_8 How concerned are you about institutions, public agencies, or intelligence services identifying you based on your online activity?

○ Not at all concerned 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ Very concerned 7

pc_types How concerned are you about the following types of information being collected and/or analyzed without your consent?

(Think about the data generated by each. For example, Streaming data would consist of usage patterns, News data would be what articles you have read, and so on).

	Not at all concerned 1	2	3	4	5	6	Very Concerned 7
Financial (1)	○	○	○	○	○	○	○
Medical (2)	○	○	○	○	○	○	○
Health, Well-being & Fitness (3)	○	○	○	○	○	○	○
Social Media (4)	○	○	○	○	○	○	○
Games (5)	○	○	○	○	○	○	○
Multimedia/Streaming (music, TV, etc.) (6)	○	○	○	○	○	○	○
News (7)	○	○	○	○	○	○	○
Lifestyle (Hobbies, Habits, Interests) (8)	○	○	○	○	○	○	○
Geographic (Location) (9)	○	○	○	○	○	○	○
Shopping/Purchases (10)	○	○	○	○	○	○	○
Photos & Video (11)	○	○	○	○	○	○	○

There can often be tensions between protecting an individual's right to privacy and the ability to collect information in order to ensure public safety. For example, access to cell phone location data is often sought after by law enforcement in order to prosecute crimes. However, individuals are often leery of having technology companies turn over information surrounding their whereabouts to law enforcement.

Thinking in a broad sense without any particular example in mind, to what extent do you agree with the following statement:

Strong individual privacy rights are detrimental to public safety.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

Section 2: Privacy and anonymity

The following section asks about your ideas surrounding privacy in relation to the idea of anonymity.

priv_anon_pref For purposes of the following question, please use the following as a guide:

Privacy refers to a situation where your identity is known, but your actions are not.
Anonymity refers to a situation where your actions are known, but your identity is not.

In each case, there is knowledge of either identity or actions, but importantly not both. As a result, anonymity is trustless (you do not need to trust the individual as you can observe/verify behavior), while privacy necessitates trust (you cannot observe/verify actions).

Within the context of the items below, indicate whether you prefer anonymity (identity unknown) or privacy (actions unknown).

	Strongly prefer anonymity (1)	Slightly prefer anonymity (2)	No preference (3)	Slightly prefer privacy (4)	Strongly prefer privacy (5)
Social media* (1)	○	○	○	○	○
Websites (2)	○	○	○	○	○
Telephone carriers (3)	○	○	○	○	○
Internet-connected devices (cameras, sensors, digital assistants, etc.) (4)	○	○	○	○	○
Public agencies or offices (5)	○	○	○	○	○
Financial transactions (6)	○	○	○	○	○
Other (specify): (7)	○	○	○	○	○

Section 3: Regulatory Environment.

The prior questions asked about your personal viewpoint on situations, regardless of what country you reside in. The next series of questions is focused on situations and conditions in your country of citizenship (${e://Field/cocit_name_embed}).

We realize that it may be difficult to disentangle a widely held societal opinion and your own, or to respond as to the prevailing opinion of an entire nation - simply answer to the best of your ability. Additionally, please note we are not asking about how things should be in that country but rather about how they are.

cocit_connection Connection to your country of citizenship (${e://Field/cocit_name_embed}).
How strong of a connection do you feel your towards your country of citizenship?

○ No Connection 1

○ 2

○ 3

○ 4

○ Very Strong Connection 5

cocit_reg1 Those that violate laws in my country of citizenship are generally held responsible.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

cocit_reg2 Regulations and laws in my country of citizenship are generally favorable to corporations.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

cocit_reg3 Law enforcement in my country of citizenship is respected and trusted.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

cocit_reg4 Regulations and laws in my country of citizenship are generally effective in achieving their stated purpose.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

cocit_reg5 Regulations and laws in my country of citizenship are generally favorable to individuals.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

Section 4: Societal Attitudes and Social structures

The following section asks about your assessment of societal ideas and attitudes in your country of citizenship (${e://Field/cocit_name_embed}).

cocit_hof_soc Think about an ideal or highly desirable job in your country of citizenship. In choosing a job in your country of citizenship, how important is it for people to:

	Of very little or no importance 1	2	3	4	Of utmost importance 5
have sufficient time for personal or home life (1)	○	○	○	○	○
have security of employment (2)	○	○	○	○	○
do work that is interesting (3)	○	○	○	○	○
have a job respected by family and friends (4)	○	○	○	○	○

cocit_soc1 Society in my country of citizenship places a high priority on individual rights and freedoms.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

cocit_soc2 Society in my country of citizenship places a high priority on collective rights.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

cocit_soc3 Society in my country of citizenship places a high priority on ideas of ownership and private property.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

cocit_soc4 In my country of citizenship, power is consolidated among a small class or group of ruling elites.

○ Do not agree at all 1

○ 2

○ 3

○ 4

○ Strongly agree 5

Distribution of Information Decision Rights.
As discussed earlier, a privacy definition that involves the ability of an individual to exercise a choice also involves the individual having the 'decision rights', or the ability to make that choice in that context, as opposed to some other entity (i.e. government, platform, corporation, etc.).

The ability to exercise choice over behaviors and actions is what is referred to by 'decision rights'.

For example, consider the decision to post on Facebook. The individual has the choice to post or not post, however Facebook as a corporation has the decision rights over what to do with information beyond the semantic meaning of the post. This includes information such as the IP address/location, time of day, browser used, and a host of other related data produced as a result of interaction with the Facebook platform.

For the following question, please think about how information decision rights are generally divided in your country of citizenship (${e://Field/cocit_name_embed}).

It may help to consider the following: *if a new technology was implemented that passively collected health/vital information from all public transport riders, who would decide how and by whom this data is used? The platform/corporation collecting or storing the data, the government, individuals, or some other entity?*

cocit_distr_decRts In your country of citizenship, how are information decision rights distributed among the following groups?

Please use the sliders to represent percentages, with the total percentage adding to 100. For example, if individuals have complete control over information that concerns them, then individuals would be 100 and all other groups would be 0. In some cases government has control over the use of information, and in other cases it could be a mix. This does not have to be precise, simply an estimate as you perceive it.

________ Individuals (1)
________ Corporations (2)
________ Government (3)
________ Other (specify): (4)

cocit_decRts_chg How would you say information decision rights (the ability to make decisions over the use of information) have changed in your country of citizenship for each of the following:

	Significantly decreased 1	2	3	Unchanged 4	5	6	Significantly increased 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and community organizations (4)	○	○	○	○	○	○	○
Other (specify): (5)	○	○	○	○	○	○	○

cocit_threat When in your Country of Citizenship, how concerned are you about the following entities/groups collecting and storing digital information about you?

	Not at all concerned 1	2	3	4	5	6	Very Concerned 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (5)	○	○	○	○	○	○	○

Section 5: Vignettes

The next section will present a series of four hypothetical scenarios, then ask the same group of questions about your possible response to each of the situations.

For each scenario, assume that you are visiting or residing in your country of citizenship (${e://Field/cocit_name_embed}) when these situations arise.

Scenario #1.
The national government approves a contract with a major corporation to connect existing video cameras located in public areas to proprietary machine learning systems that utilize facial recognition technology trained to recognize an individual's emotional state. The announcement explains that this data will only be used to assist law enforcement in identifying persons of interest for crimes that currently have no leads or suspects.

Assume you are visiting or residing in your country of citizenship as this scenario unfolds.

v1_entity Which entity would you expect to have primary decision rights (the ability to make decisions about the use of information) regarding the information generated in this scenario?

○ Individuals

○ Corporations

○ Government

○ Non-profit and/or community organizations

○ Other (specify): ____

○ I don't know

v1_distrChg How would the scenario above affect the information decision rights (the ability to make decisions about the use of information) for each of the following:

	Significantly Decrease 1	2	3	No Change 4	5	6	Significantly Increase 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (5)	○	○	○	○	○	○	○

v1_privDesire How would this scenario affect your desire for information privacy?
(Information privacy: control over information that regulates access to the self in order to enhance current and future decision and behavioral choice)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v1_anonDesire How would this scenario affect your desire for digital anonymity?
(digital anonymity: ability to remain unidentifiable in collections of digital information)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v1_behavior Which of the following approaches would you adopt in such a situation? (Mark all that apply).

□ I would discuss the situation with family, friends, and/or colleagues.

□ I would seek to limit the use and disclosure of my information that is collected and stored.

□ I would attempt to avoid my information from being collected in the first place.

□ Other (specify): ____

□ ⊗I would do nothing.

v1_threat How concerned would you be about the following entities/groups in relation to digital information collected about you as a result of the changes described in this scenario?

	Not at all concerned 1	2	3	4	5	6	Very Concerned 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (8)	○	○	○	○	○	○	○

Scenario #2.
A biotech firm unveils new technology whereby a small (thumbnail-sized), flexible patch is able to adhere to an individual's skin and provide real-time monitoring of an individual's organs, tissues, and blood chemistry. Initial marketing of the devices is geared towards consumers, with a phone app available to connect to the sensors in order to view and track information. The data can be used upstream to

reconstruct images of soft tissue, analyze blood chemistry, and provide personalized medical recommendations.

Assume you are visiting or residing in your country of citizenship as this scenario unfolds.

v2_entity Which entity would you expect to have primary decision rights (the ability to make decisions about the use of information) regarding the information generated in this scenario?

○ Individuals

○ Corporations

○ Government

○ Non-profit and/or community organizations

○ Other (specify): ____

○ I don't know

v2_distrChg How would the scenario above affect the information decision rights (the ability to make decisions about the use of information) for each of the following:

	Significantly Decrease 1	2	3	No Change 4	5	6	Significantly Increase 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (5)	○	○	○	○	○	○	○

v2_privDesire How would this scenario affect your desire for information privacy?
(Information privacy: control over information that regulates access to the self in order to enhance current and future decision and behavioral choice)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v2_anonDesire How would this scenario affect your desire for digital anonymity?
(digital anonymity: ability to remain unidentifiable in collections of digital information)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v2_behavior Which of the following approaches would you adopt in such a situation? (Mark all that apply).

□ I would discuss the situation with family, friends, and/or colleagues.

□ I would seek to limit the use and disclosure of my information that is collected and stored.

□ I would attempt to avoid my information from being collected in the first place.

□ Other (specify): ____

□ ⊗I would do nothing.

v2_threat How concerned would you be about the following entities/groups in relation to digital information collected about you as a result of the changes described in this scenario?

	Not at all concerned 1	2	3	4	5	6	Very Concerned 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (8)	○	○	○	○	○	○	○

Scenario #3.

Regulations governing corporate charters are amended to expand corporate responsibilities beyond financial/fiduciary duties to include elements of responsible data management. Corporations can now be held liable not only for financial mismanagement, but also for data mismanagement or negligence. Best practices include principles of minimal required collection (collect only information that has a clear identified purpose and will not pose an outsized risk), data expiration and deletion, and clearly delineated processes for identifying and managing data risk.

Assume you are visiting or residing in your country of citizenship as this scenario unfolds.

v3_entity Which entity would you expect to have primary decision rights (the ability to make decisions about the use of information) regarding the information generated in this scenario?

○ Individuals

○ Corporations

○ Government

○ Non-profit and/or community organizations

○ Other (specify): ____

○ I don't know

v3_distrChg How would the scenario above affect the information decision rights (the ability to make decisions about the use of information) for each of the following:

	Significantly Decrease 1	2	3	No Change 4	5	6	Significantly Increase 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (5)	○	○	○	○	○	○	○

v3_privDesire How would this scenario affect your desire for information privacy?

(Information privacy: control over information that regulates access to the self in order to enhance current and future decision and behavioral choice)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v3_anonDesire How would this scenario affect your desire for digital anonymity?
(digital anonymity: ability to remain unidentifiable in collections of digital information)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v3_behavior Which of the following approaches would you adopt in such a situation? (Mark all that apply).

□ I would discuss the situation with family, friends, and/or colleagues.

□ I would seek to limit the use and disclosure of my information that is collected and stored.

□ I would attempt to avoid my information from being collected in the first place.

□ Other (specify): ____

□ ⊗I would do nothing.

v3_threat How concerned would you be about the following entities/groups in relation to digital information collected about you as a result of the changes described in this scenario?

	Not at all concerned 1	2	3	4	5	6	Very Concerned 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (8)	○	○	○	○	○	○	○

Scenario #4.
The national government adopts national data standardization practices that require corporations transmitting data digitally to include certain pieces of information (metadata) that allow the government to identify and organize it. The government makes use of existing access to primary internet cables entering and exiting the country in combination with the new metadata to collect and archive corporate data in an effective and organized manner. The effort is promoted as a response to corporate espionage aimed at protecting national corporate secrets as well as safeguarding information that corporations are

entrusted with.

Assume you are visiting or residing in your country of citizenship as this scenario unfolds.

v4_entity Which entity would you expect to have primary decision rights (the ability to make decisions about the use of information) regarding the information generated in this scenario?

○ Individuals

○ Corporations

○ Government

○ Non-profit and/or community organizations

○ Other (specify): ____

○ I don't know

v4_distrChg How would the scenario above affect the information decision rights (the ability to make decisions about the use of information) for each of the following:

	Significantly Decrease 1	2	3	No Change 4	5	6	Significantly Increase 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (5)	○	○	○	○	○	○	○

v4_privDesire How would this scenario affect your desire for information privacy?
(Information privacy: control over information that regulates access to the self in order to enhance current and future decision and behavioral choice)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v4_anonDesire How would this scenario affect your desire for digital anonymity?
(digital anonymity: ability to remain unidentifiable in collections of digital information)

○ Significantly Decrease 1

○ 2

○ 3

○ No Change 4

○ 5

○ 6

○ Significantly Increase 7

v4_behavior Which of the following approaches would you adopt in such a situation? (Mark all that apply).

□ I would discuss the situation with family, friends, and/or colleagues.

□ I would seek to limit the use and disclosure of my information that is collected and stored.

□ I would attempt to avoid my information from being collected in the first place.

□ Other (specify): ____

□ ⊗I would do nothing.

v4_threat How concerned would you be about the following entities/groups in relation to digital information collected about you as a result of the changes described in this scenario?

	Not at all concerned 1	2	3	4	5	6	Very Concerned 7
Individuals (1)	○	○	○	○	○	○	○
Corporations (2)	○	○	○	○	○	○	○
Government (3)	○	○	○	○	○	○	○
Non-profit and/or community organizations (4)	○	○	○	○	○	○	○
Other (specify): (8)	○	○	○	○	○	○	○

Demographic Information.

The following questions ask basic demographic information, you are free to skip any questions you do not wish to answer.

What is your age?

- ○ 24 or younger
- ○ 25-29
- ○ 30-34
- ○ 35-39
- ○ 40-49
- ○ 50-59
- ○ 60 or above
- ○ Decline to State

What is your gender?

- ○ Male
- ○ Female
- ○ Non binary
- ○ Decline to State

Finally, this project will also include an online focus group session of approximately 3-5 individuals to dive deeper into some of these topics. The online session will be recorded for data analysis purposes, but participants will not be asked to identify themselves.

Are you interested in participating in an online focus group?

- ○ Yes, I am interested in participating in an online focus group.
- ○ No.

Appendix B: Supplemental tables

Table B.1. Initial IPC Cronbach's alpha, prior to removal of item Q27.R (privacy is detrimental to public safety).

IPC Construct Item	*n*	*raw.r*	*std.r*	*r.cor*	*r.drop*	*mean*	*sd*
privconc_overall	32	0.81	0.81	0.81	0.75	4.6	1.6
pc1_Mas_v1	32	0.82	0.83	0.83	0.77	5.1	1.5
pc2_Mas_v2	32	0.83	0.84	0.83	0.79	5.7	1.3
pc3_Mas_v3	32	0.82	0.82	0.81	0.76	5.3	1.6
pc6	32	0.82	0.83	0.81	0.77	5.6	1.4
pc4_Mas_v4	32	0.77	0.76	0.74	0.69	5.3	1.8
pc5_Mas_v5	32	0.79	0.79	0.78	0.74	5.2	1.4
pc_7	32	0.77	0.75	0.74	0.69	4.6	1.6
pc_8	32	0.86	0.85	0.85	0.82	5.4	1.5
Q27.R	32	-0.15	-0.13	-0.23	-0.26	2.7	1.3

Table B.2. Model H2-a regression results

	Estimate	*Std. Error*	*t value*	*Pr(>|t|)*
(Intercept)	5.0521	1.2584	4.0150	0.0004***
cocit_distr_decRts_1	0.0199	0.0166	1.1980	0.2413
cocit_distr_decRts_2	-0.0312	0.0277	-1.1270	0.2695
cocit_distr_decRts_3	NA	NA	NA	NA
reg.c	-0.3961	0.2796	-1.4170	0.1681
soc.c	0.2277	0.3531	0.6450	0.5246

Table B.3. Model H2-a correlations

	cocit_distr_decRts_1	*cocit_distr_decRts_2*	*cocit_distr_decRts_3*	*reg.c*	*soc.c*
cocit_distr_decRts_1	1.0000	0.0341	-0.8472	0.2548	0.4292
cocit_distr_decRts_2	0.0341	1.0000	-0.5598	-0.2881	0.3294
cocit_distr_decRts_3	-0.8472	-0.5598	1.0000	-0.0581	-0.5309
reg.c	0.2548	-0.2881	-0.0581	1.0000	0.3551

soc.c	0.4292	0.3294	-0.5309	0.3551	1.0000

References

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

Adjerid, I., Peer, E., and Acquisti, A. 2018. “Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making,” Mis Quarterly (42:2), Minneapolis: Soc Inform Manage-Mis Res Cent, pp. 465-+. (https://doi.org/10.25300/MISQ/2018/14316).

Akerlof, G. A. 1970. “The Market for ‘Lemons’: Quality Uncertainty and the Market Mechanism,” Quarterly Journal of Economics (84:3), Oxford University Press / USA, pp. 488–500. (https://doi.org/10.2307/1879431).

Al-Natour, S., Cavusoglu, H., Benbasat, I., and Aleem, U. 2020. “An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps,” Information Systems Research (31:4), Catonsville: Informs, pp. 1037–1063. (https://doi.org/10.1287/isre.2020.0931).

Arendt, H., and Canovan, M. 1998. The Human Condition. 2nd ed. Chicago: University of Chicago Press.

Baruh, L., & Cemalcılar, Z. 2014. “It is more than personal: Development and validation of a multidimensional privacy orientation scale,” Personality and Individual Differences, 70, 165-170.

Bansal, G., Zahedi, F. “Mariam,” and Gefen, D. 2015. “The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern,” European Journal of Information Systems (24:6), Abingdon: Taylor & Francis Ltd, pp. 624–644. (https://doi.org/10.1057/ejis.2014.41).

Belanger, F., and James, T. L. 2020. “A Theory of Multilevel Information Privacy Management for the Digital Era,” Information Systems Research (31:2), Catonsville: Informs, pp. 510–536. (https://doi.org/10.1287/isre.2019.0900).

Belanger, F., and Crossler, R. E. 2011. “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems,” Mis Quarterly (35:4), Minneapolis: Soc Inform Manage-Mis Res Cent, pp. 1017–1041.

Belanger, F., and Crossler, R. E. 2019. “Dealing with Digital Traces: Understanding Protective Behaviors on Mobile Devices,” Journal of Strategic Information Systems (28:1), Amsterdam: Elsevier, pp. 34–49. (https://doi.org/10.1016/j.jsis.2018.11.002).

Belanger, F., and Xu, H. 2015. “The Role of Information Systems Research in Shaping the Future of Information Privacy,” Information Systems Journal (25:6), Hoboken: Wiley-Blackwell, pp. 573–578. (https://doi.org/10.1111/isj.12092).

Benjamin, V., Valacich, J. S., and Chen, H. 2019. “Dice-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics,” Mis Quarterly (43:1), Minneapolis: Soc Inform Manage-Mis Res Cent, pp. 1–22. (https://doi.org/10.25300/MISQ/2019/13808).

Burton, A., Scott, S. V., Butler, B. S., and Xu, S. X. 2021. “Next-Generation Information Systems Theorizing: A Call-to-Action,” Mis Quarterly, p. 20.

Caughlin, D. E. 2022. R for HR: An Introduction to Human Resource Analytics Using R, Self-Published, Version 0.1.2: 2022-07-13. https://rforhr.com/, accessed 5/1/2023.

Crawford, K. 2021. “Time to Regulate AI That Interprets Human Emotions,” Nature (592:7853), Nature Publishing Group, pp. 167–167. (https://doi.org/10.1038/d41586-021-00868-5).

Dinev, T. 2014. “Why Would We Care about Privacy? Introduction,” European Journal of Information Systems (23:2), Abingdon: Taylor & Francis Ltd, pp. 97–102. (https://doi.org/10.1057/ejis.2014.1).

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. “Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the ‘APCO’ Box,” Information Systems Research (26:4), Catonsville: Informs, pp. 639–655. (https://doi.org/10.1287/isre.2015.0600).

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. “Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts,” European Journal of Information Systems (22:3), Abingdon: Taylor & Francis Ltd, pp. 295–316. (https://doi.org/10.1057/ejis.2012.23).

Hair, J. F., Hult, G.T.M., Ringle, C. M., & Sarstedt, M. 2017. A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). Thousand Oaks: Sage.

Hair, J. F., Ringle, C.M., Gudergan, S.P. et al. 2019. “Partial least squares structural equation modeling-based discrete choice modeling: an illustration in modeling retailer choice,” Bus Res 12, 115–142. https://doi.org/10.1007/s40685-018-0072-4

Hair, J. F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., Danks, N.P., Ray, S. 2021. Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R. Classroom Companion: Business. Springer, Cham. (https://doi.org/10.1007/978-3-030-80519-7)

Hair, J. F., Hult, G.T.M., Ringle, C. M., & Sarstedt, M. (2022). A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.). Thousand Oaks: Sage.

Henseler, J., Ringle, C.M. & Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. of the Acad. Mark. Sci.* 43, 115–135 (2015). https://doi.org/10.1007/s11747-014-0403-8

Hofstede, G. 2013. VSM 2013: Values Survey Module 2013 English language version. https://geerthofstede.com/wp-content/uploads/2016/07/VSM-2013-English-2013-08-25.pdf, accessed 5/13/2022.

Hothorn T, Bretz F, Westfall P (2008). "Simultaneous Inference in General Parametric Models." Biometrical Journal, 50(3), 346–363.

Hovorka, D. S., and Peter, S. 2021. "Speculatively Engaging Future(s): Four Theses," MIS Quarterly (45:1), pp. 461–466.

Kass, L. 2002. Life Liberty & the Defense of Dignity: The Challenge for Bioethics, New York, United States: Encounter Books.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," Information Systems Journal (25:6), Hoboken: Wiley, pp. 607–635. (https://doi.org/10.1111/isj.12062).

Kvasny, L., and Keil, M. 2006. "The Challenges of Redressing the Digital Divide: A Tale of Two US Cities," Information Systems Journal (16:1), pp. 23–53. (https://doi.org/10.1111/j.1365-2575.2006.00207.x).

Leidner, D. E., and Tona, O. 2021. "The Care Theory of Dignity Amid Personal Data Digitalization," MIS Quarterly (45:1), MIS Quarterly, pp. 343–370. (https://doi.org/10.25300/MISQ/2021/15941).

Lohmoller, J. 1989. Latent Variable Path Modeling with Partial Least Squares. Physica-Verlag, Heidelberg. (https://doi.org/10.1007/978-3-642-52512-4)

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

Margulis, S. T. 2003. “On the Status and Contribution of Westin’s and Altman’s Theories of Privacy,” Journal of Social Issues (59:2), Wiley-Blackwell, pp. 411–429. (https://doi.org/10.1111/1540-4560.00071).

Marshall, D., and Thomas, T. 2017. Privacy and Criminal Justice, Cham: Springer International Publishing. (https://doi.org/10.1007/978-3-319-64912-2).

Masur, P. K. 2018. Situational privacy and self-disclosure: Communication processes in online environments. Cham, Switzerland: Springer. doi: 10.1007/9783-319-78884-5

Miltgen, C. L., and Peyrat-Guillard, D. 2014. “Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries,” European Journal of Information Systems (23:2), Abingdon: Taylor & Francis Ltd, pp. 103–125. (https://doi.org/10.1057/ejis.2013.17).

Oetzel, M. C., and Spiekermann, S. 2014. “A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach,” European Journal of Information Systems (23:2), Abingdon: Taylor & Francis Ltd, pp. 126–150. (https://doi.org/10.1057/ejis.2013.18).

Ozdemir, Z. D., Smith, H. J., and Benamati, J. H. 2017. “Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study,” European Journal of Information Systems (26:6), Abingdon: Taylor & Francis Ltd, pp. 642–660. (https://doi.org/10.1057/s41303-017-0056-z).

Pavlou, P. A. 2011. “State of the Information Privacy Literature: Where Are We Now and Where Should We Go?,” Mis Quarterly (35:4), Minneapolis: Soc Inform Manage-Mis Res Cent, pp. 977–988.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective,” Mis Quarterly (31:1), Minneapolis: Soc Inform Manage-Mis Res Cent, pp. 105–136.

Posner, R. A. 1978. “An Economic Theory of Privacy,” Regulation, p. 9.

R Core Team (2020). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/.

Ray, S., and Danks, N. 2021. *SEMinR: Building and Estimating Structural Equation Models.* R package version 2.3.2, https://cran.r-project.org/package=seminr.

Revelle, W. (2023). *psych: Procedures for Psychological, Psychometric, and Personality Research.* Northwestern University, Evanston, Illinois. R package version 2.3.3, https://CRAN.R-project.org/package=psych.

Riemer, K., Ciriello, R., Peter, S., and Schlagwein, D. 2020. “Digital Contact-Tracing Adoption in the COVID-19 Pandemic: IT Governance for Collective Action at the Societal Level,” European Journal of Information Systems (29:6), Abingdon: Taylor & Francis Ltd, pp. 731–745. (https://doi.org/10.1080/0960085X.2020.1819898).

Rosch, E. 1973. “Natural Categories,” Cognitive Psychology (4:3), Academic Press, pp. 328–350. (https://doi.org/10.1016/0010-0285(73)90017-0).

Royakkers, L., Timmer, J., Kool, L., and van Est, R. 2018. “Societal and Ethical Issues of Digitization,” Ethics and Information Technology (20:2), pp. 127–142. (https://doi.org/10.1007/s10676-018-9452-x).

Rule, J. B. 1974. Private Lives and Public Surveillance; Social Control in the Computer Age, New York: Schocken Books.

Smith, H. J., Dinev, T., and Xu, H. 2011. “Information Privacy Research: An Interdisciplinary Review,” Mis Quarterly (35:4), Minneapolis: Soc Inform Manage-Mis Res Cent, pp. 989–1015.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices,” MIS Quarterly (20:2), Management Information Systems Research Center, University of Minnesota, pp. 167–196. (https://doi.org/10.2307/249477).

Soetewey, A. 2020. “Stats and R”. url: https://statsandr.com/blog/anova-in-r, accessed 5/13/2023.

Spiekermann, S., and Korunovska, J. 2017. “Towards a Value Theory for Personal Data,” Journal of Information Technology (32:1), London: Sage Publications Ltd, pp. 62–84. (https://doi.org/10.1057/jit.2016.4).

Warren, S., and Brandeis, L. 1890. “The Right to Privacy,” Harvard Law Review (4:5), pp. 193–220.

Whitley, E. A., Gal, U., and Kjaergaard, A. 2014. “Who Do You Think You Are? A Review of the Complex Interplay between Information Systems, Identification and Identity,” European Journal of Information Systems (23:1), Abingdon: Taylor & Francis Ltd, pp. 17–35. (https://doi.org/10.1057/ejis.2013.34).

Xue, Y., Liang, H., and Boulton, W. R. 2008. “Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context,” Mis Quarterly (32:1), Minneapolis: Soc Inform Manage-Mis Res Cent, pp. 67–96.

Zuboff, S. 2015. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” Journal of Information Technology (30:1), London: Sage Publications Ltd, pp. 75–89. (https://doi.org/10.1057/jit.2015.5).

Zwick, D., and Dholakia, N. 2004. “Consumer Subjectivity in the Age of Internet: The Radical Concept of Marketing Control through Customer Relationship Management,” Information and Organization (14:3), pp. 211–236. (https://doi.org/10.1016/j.infoandorg.2004.01.002).