Click "Accept"

Exploring justification & responsibility in unravelling the 'privacy paradox'

Ryan Morgan

Student Number: 508015

Supervisor: Julian Schaap

16 June 2019

10980 words

Click “Accept”: Exploring justification & responsibility within the ‘privacy paradox’

Abstract

In 2018, global media coverage of data privacy issues peaked in the wake of successive Facebook and Google privacy scandals. As state and corporate actors engaged in discourse on the issue, individual actors, or the 'user class', were left out. In light of traditional privacy research, this was understandable, as individuals have historically demonstrated inconsistencies in their attitudes and behaviours surrounding data privacy. This phenomenon is the privacy paradox, wherein users express concerns for the privacy of their data but regularly act or behave in ways that undermine or fail to protect it. However, is this the whole story? Moreover, in an era of increased technological penetration and decreasing privacy, can users afford to be silent within a potentially false paradox? This thesis argues that the privacy paradox is a result of reductionist approaches to the study of privacy and aims to demonstrate that user conceptualisations surrounding data privacy are not as paradoxical as supposed.

Through the construction of a context-integrity framework, integrated with an analytical application of regimes of justification, consistent patterns of contextual influence within user data privacy conceptualisations were exposed. Identified via semi-structured interviews (n=20) with Dutch and American individual users these patterns proved to be coherent, measurable, and predictable across contexts, surpassing the limitations of traditional reductionist measures that fail to reconcile user attitudes and behaviours. This research contributes to an enhanced understanding of complex, norm-sensitive issues such as data privacy, increasingly relevant when technological and corporate influences on privacy norms are steadily increasing.

Keywords: context-integrity; data privacy; norm entrepreneurship; privacy paradox; regimes of justification

Introduction

At the turn of the new year, proclamations that 2018 had been “the year of data protection” (Laskai, 2019) rang out across the internet. From the dark corners of the blogosphere to the main pages of the most popular tech-forums, many claimed that the issue of data privacy had finally secured its proper place on the public agenda. Such assertions certainly seemed warranted, as the end of 2018 saw the governments of the United States and China begin independent discussions of historic regulatory legislation, against the expressed interests of corporations such as Google, Amazon, and Alibaba (Cyphers et al., 2018). Other nations, as well as some American states, also began independently confronting tech giants, emboldened by the promises surrounding the EU's General Data Protection Regulation (instituted May 2018). Concerned for the fallout from seemingly weekly parades of new data privacy scandals, state regulators across the globe appeared on track to put users/consumers into a position to take back data privacy control, slowing the global march of Big Data.

Thirteen months on from the effective date of the GDPR, however, little has changed for users. Discussions of the GDPR have turned away from promises of user benefits to focus on the increasing costs of compliance (Rand, 2019; Forbes Technology Council, 2018). Although several major corporations have announced data privacy-focused projects (e.g. Apple sign -in (Brandom, 2019), Microsoft ION (Barber, 2019)), discussions of data privacy and regulation are still dominated exclusively by state & corporate actors. As a result, reforms have stalled as Silicon Valley CEOs and tech-interest groups pressure legislators to regulate within industry defined terms (Carr, 2018). Despite continued scandals (Singh, 2019) and the failure of post-GDPR regulation promises to come to swift fruition, users nonetheless continue to willingly generate and disclose information, at increasing rates, despite rising privacy concerns and the growing public attention on data protection issues (Rainie, 2018).

This discrepancy between user concerns and disclosure behaviours represents a “privacy paradox” (Nordberg et al., 2007; Gerber et al., 2018). Though users often express concern regarding the privacy of their personal information, statistical studies repeatedly show these concerns rarely correlate with protective actions and disclosure behaviors. To typify this paradoxical behaviour, a 2017 Pew Research Survey reported that while 41% of Americans had encountered fraudulent charges on credit cards, 41% of online adults had shared at least one password with a friend or family member, and 35% admitted to using the same or very similar passwords for multiple online accounts (Smith, 2017). Users also freely disclose personal data often by posting private details to social media networks and using personal fitness trackers and e-commerce sites (Gerber et al., 2018).

The extant literature exploring this phenomenon does so predominantly through quantitative survey and summative scale analyses, aimed at answering a number of fundamental questions: *why do users engage in these paradoxical behaviours, what kinds of attitudes lead users to behave incongruously with their intentions,* and *what behaviours predict when users will disregard their privacy concerns* (Gerber et al., 2018).

There are two current limitations inherent to this body of research. The first is that the majority of such studies rely on traditional conceptions of privacy (Norberg et al., 2007), notions that focus on the legal language of control and access. In their individualistic focus, such notions have struggled to explain attitudes and behaviours in the connectedness of contemporary data privacy environments, where participation is contingent upon sharing (Marwick & boyd, 2014). The second limitation derives from the common assumption that individuals perceive themselves to be the most responsible actors for data privacy. Such an assumption drives privacy researchers to focus heavily on superficial indicators such as externally-directed levels of trust and risk

(Gerber et al., 2018), while often ignoring the surrounding contextual details such as internal motivations or environmental incentives. For example, a teenager’s decision to post pictures of their first car to Facebook cannot solely be a result of the levels of trust and risk they associate with the platform. Social capital, the esteem gained from friends, or the pride felt in reaching a cultural milestone may be far more influential factors, but they fall into a category of data omitted from traditional data privacy surveys.

This thesis confronts these limitations and their inherent reductionism, by exploring the following research questions: *How do individuals perceive agency and responsibility regarding data privacy? How do individuals construct justifications for these perceptions? How do these constructed justifications differ across cultural contexts?* Through semi-structured interviews (*n* = 20), this research aims to integrate a context-integrity framework with an analytical application of ‘regimes of justification’ to bring resolution to the privacy paradox by exposing patterns of consistent contextual influences underpinning attitudes, behaviors, and associated conceptualisations surrounding data privacy among American and Dutch citizens.

Both the social and scientific relevance for such research is growing. As the ‘datafication’ (van Dijck, 2014) of society progresses and *norm-entrepreneurship*—the intentional shaping of societal norms—becomes an increasingly attractive and relevant pursuit within the technology sector, it is imperative that individuals, academics, corporations and policy-makers invest in understanding norms, how different actors perceive these norms, and how these actors construct different ways of adapting when these norms change.

The aim of this research is to provide two things: a design framework that successfully exposes the underlying contexts of a complex, norm-sensitive privacy phenomena, and an exploration of the patterns of argumentation individuals construct when dealing with the

difficulties of conceptualising data privacy. The potential gains are two-fold: a previously overlooked yet theoretically fundamental area for data privacy research opens, and the nature of the relationship between individuals and the data they generate (across myriad contexts) is exposed, benefiting academic and policy-making communities in contributing to an enhanced understanding of our shared data privacy environment.

The body of this thesis is divided into three primary sections. First, the theoretical framework section addresses the disparities between traditional and contextual notions of privacy and introduces the key theoretical notions of Nissenbaum’s ‘framework of context-integrity’ (2010) and Boltanski & Thévenot's (2006) 'regimes of justification'. Subsequently, the methods & data section outlines the integrated interview design, as well as the data collection and analysis processes. Lastly, the results are presented in three parts. The first highlights users’ argumentations legitimising their personal or ‘ideal’ conceptions of privacy. This is followed by a presentation of argumentations users constructed when confronted with ‘reality’ or competing regimes. The third part consists of a brief comparative look at the different patterns constructed between participants. The three primary sections are followed by a conclusion, including discussion of results, limitations and implications.

Theoretical Framework

Privacy: Traditional vs Contextual

The enduring distinction underpinning traditional notions of privacy demarcates what is considered private from what is considered public, with much the same rigidity that a concrete curb divides that which is one’s private driveway from that which is a public street. Though social scientists have argued against such a distinction in favour of more contextual notions (Marwick & boyd, 2014), much of how Western societies collectively understand and define

privacy remains rooted in this rigidity, commonly expressed through a public/private dichotomy. However, recent research has highlighted contemporary contextual challenges to this traditional dichotomy—challenges that posit the private/public as a concept more negotiated than demarcated. The popularity of such notions has swiftly increased alongside a renewed interest in privacy studies; a consequence of the unique sociological challenges posed by the meteoric rise of 'networked publics', the 'Internet of Things (IoT)', 'Big Data', and 'datafication' (boyd & Crawford, 2012; Marwick & boyd, 2014; Nippert-Eng, 2010; Nissenbaum, 2010; Tufekci, 2017; van Dijck, 2014).

The most consistently presented challenge highlights the inability of traditional privacy conceptions to adequately address the nature of privacy as it is practiced in contemporary “networked publics” (Marwick & boyd, 2014). Nippert-Eng (2010) elegantly captures these realities in the metaphor of “beaches” on “islands of privacy” (pp. 10-11). This metaphor frames individual attempts to balance “selective concealment and disclosure” as management of the shifting topography between an “island of privacy” and an “ocean of publicness” (Nippert-Eng, 2010, p. 11). Just as shorelines are ever in a state of flux, so do conceptions of what is private or public ebb and flow with the contextual tides of these networked publics.

Data Privacy Protection

Many privacy scholars argue that the “datafication” of daily life (van Dijck, 2014), resulting from the inescapable growth and pervasive penetration of Internet of Things (IoT), Big Data, and social media technologies, poses unique threats to privacy—“shrinking our islands” (Nippert-Eng, 2010, p. 3) and reframing the management of our ‘beaches’. As a result, what was once only a narrow strip along a broader shore, data privacy has quickly become the most salient of

privacy concerns in the public discourse (Viveiros, 2018). However, what is it that truly threatens the privacy of data, and what precisely is to be feared?

Privacy Violations

Because traditional conceptions of privacy are inadequate for managing the contemporary realities of privacy practice, it is reasonable to presume that such rigid notions are also inadequate for conceptualising contemporary privacy threats; particularly those threats arising from the increased interconnectedness of social networks and data collection. Here, Helen Nissenbaum's (2010) ‘framework of contextual integrity’ provides a capable alternative for understanding contextual privacy and threats to data privacy.

Traditional approaches to privacy concerns are based on “simplistic models of individual behavior”, even though modern societies are constructed from “webs of cultural and material connections” (Cohen, 2012, pp. 4-5). These simplistic models ground privacy in measures of an individual’s control over information or their ability to restrict access to it, a perspective Nissenbaum directly challenges with her framework. According to her framework, in the interconnectedness of contemporary publics, concern for privacy originates *not* from a desire to control information flow, but rather from a desire to ensure that it flows “appropriately” (Nissenbaum, 2010).

The appropriateness of information flow anchors the notion of ‘context-integrity’. According to this framework, finely tuned systems of social norms and rules—referred to as “context-relative informational norms”—govern personal information flow in specific social contexts (p. 3). These norms define important activities, key relationships and interests, and they “protect people and groups”. They are also “responsive to historical, cultural and even geographic contingencies” in that they form distinct patterns from one society to the next (p. 3).

There are four components or 'parameters' that characterise these norms: *contexts*, *actors*, *attributes*, and *transmission principles*. Fundamental to structuring the framework, these parameters generally specify for a given context the information type, the subjects, the senders and receivers, and the "principles under which this information is transmitted" (Nissenbaum, 2010, pp. 140-141). Within this framework, the threat of privacy violation is understood as the *transgression* of the context-integrity of relevant informational norms along one or more parameters, contradicting traditional individualistic conceptions of violations as simply an acute loss of control, failure to prohibit access, or an imbalance of trust and risk. This distinction in the nature of privacy violation poses significant implications for understanding the dominant contemporary data privacy discourse.

Protection: Strategy & Responsibility

As noted in the introduction, following a swift and continued rise in salience, concern for data privacy violations recently topped global public agendas as players across all levels of responsibility (individual, corporate, state) seek to minimise occurrences. Corporations and states share a vested interest in the minimisation of privacy violations: by diminishing negative consequences to public sharing patterns they ensure the continuance of Big Data markets and the expansion of consumer data collection environments. These actors currently dominate the data privacy discourse and while they may approach data privacy with a common strategy, they execute it by taking up the counterbalancing responsibilities of innovation and regulation.[1] Through this generally iterative cycle of innovation-regulation, both actors compete as "norm entrepreneurs" (Sunstein, 1996) to shape public attitudes in favour of an inverse relationship of

[1] Two exceptions to this general corporate/innovator to state/regulator relationship, are the interpretation of the EU GDPR as 'innovation' in the realm of data privacy regulation, and the recent unprecedented push of Apple's Tim Cook, and Facebook, to generate privacy standards regulation independently.

increased sharing and decreased privacy. As corporations introduce new data technologies, techniques and practices, states seek to balance the social impacts through regulation and policy, and this purposeful shaping of social norms can be considered “norm entrepreneurship” (IoT Privacy Forum, 2018).

Individual actors, of course, seek to minimise the occurrence of violations as well. At this level, however, perceptions of strategy and responsibility are historically ambiguous. Two observations frame this ambiguity: a consistent reliance on the language of traditional privacy conceptions (i.e. control, access, trust, risk), and the resulting privacy paradox (Gerber et al., 2018; Norberg et al., 2007).

From these observations, individual actors appear to strategically claim certain authorities (language), while not taking upon themselves any distinct responsibilities in the manner that corporate and state actors do (paradox), ultimately demonstrating a conflict between a sense of inherent possession of privacy rights and a lack of inherent ability to secure them. The resulting strategic disparity, between the ‘norm entrepreneurship’ of state and corporate actors, and individual actors’ seemingly empty claims to traditional privacy notions, makes impossible a general consensus on where conceptualisations of data privacy and associated responsibilities begin or end. In making either competing or conflicting claims to both authority and responsibility, the triad of actors leave significant elements undefined and unassigned. As a result, the contextual influences informing user conceptions of data privacy and associated responsibilities go unconsidered, in favour of popular measures of externally-directed considerations of control and access, trust and risk—reductionist captures of individual user reactions to the voices and interests of the dominant actors (state and corporate). Because these contextual influences remain mostly unexplored or ignored, individual actors are seemingly left

to mire silently in a paradoxical phenomenon regarded as self-constructed, with no voice to participate in the larger discourse.

Resolution

Theoretically, however, the seemingly conflicted and ambiguous contexts surrounding individual data privacy conceptualisations can be rescued from the paradox through what is here referred to collectively as ‘resolution’, in the sense that it is a process addressing both contextual determinacy and empirical clarity. This process for resolving *how* and *why* individuals conceptualise data privacy in certain ways, as well as *under what contexts* they do so, occurs in two steps.

Resolution: Context Integrity

The first step towards resolution is incorporating the principle of context-integrity to unravel the privacy paradox. As a distinct collective, relative to states and corporations, individuals demonstrate incongruity both in claiming authorities yet disclaiming responsibilities (regarding their own intentions and behaviours) and in denying authorities yet projecting responsibilities (regarding traditional notions of privacy). This incongruity is the classic perception of the paradox phenomenon. This incongruity begins to disappear, however, when ample context is exposed to support individual user conceptualisations, exceeding traditional limitations. According to Nissenbaum (2010), “because contextual integrity demands appropriate flow and not merely control and secrecy, it predicts the behaviors skeptics cite as paradoxical” (p. 15). For contextual privacy scholars such as Marwick, boyd, and Nippert-Eng,

> "If a right to privacy is a right to *context-appropriate* flows, and not to secrecy or to control over information about oneself, there is no paradox in caring deeply about privacy and, at the same time, eagerly sharing information as long as the sharing and withholding

> conform with the principled conditions prescribed by governing contextual norms." (Nissenbaum, 2010, p. 187)

As a result, the perceived paradox becomes irrelevant when approaching data privacy from a framework of context-integrity, as the framework grounds exploration and exposure of the parameters along which individual perceptions of agency and responsibility shift, in relative contextual terms. This clarity is prerequisite to the second step in the process of resolution.

Resolution: Regimes of Justification

The context-integrity framework accommodates and expects plurality in the *how* and *why* that surrounding individual conceptualisations of data privacy. An equally open and capable structure is then required for exploring user determinations of appropriateness, or what does or does not constitute legitimacy for specific conceptualisations. Well-suited for this task is the pluralistic approach to understanding argumentation found in Boltanski and Thévenot's (2006) 'regimes of justification'.

Boltanski and Thévenot (2006), in their seminal work “On Justification” argue that in any specific situation, individuals are likely to mobilise multiple argumentations in seeking legitimacy for themselves. In this theoretical framework, justifications include interrelated supportive arguments, claims of worth, compromises and “critical denunciations of opposing views” or critiques (Arts et al., 2018, p. 1072). Individual actors mobilise these different ‘regimes of justification’, “each with its own way of separating good from bad, right from wrong, just from unjust” (Arts et al., 2018, p. 1072), to stabilise uncertainties and establish or dispute legitimacy.

There are six different regimes, according to Boltanski and Thévenot (2006), and one additional regime subsequently theorised by Boltanski and Chiappello. The original six are the

industrial, *fame*, *domestic*, *civic*, *market*, and *inspired* regimes; the additional (seventh) regime is the *network* regime (Boltanski & Chiappello, 2005). Each regime is based upon a different evaluative principle of worth, linking within each regime justifications legitimising or delegitimising constructed argumentations.

In the *industrial* regime, worth derives from notions of efficiency. Individuals seeking legitimacy construct justifications supporting progress and growth; they value things that have a specific use or a proper function, things that are (perceived to be) under their control and contribute to a predictable future that can be measured in some way. For example, the *industrial* regime is typically mobilised when actors use navigation apps such as Waze or Google Maps. These apps require voluntary disclosure of exact user location data. The loss of privacy is justified here in the efficiency the user gains by taking faster routes that avoid traffic and other obstacles. Traditional expressions of having control over information can sometimes be understood to originate in this regime, but only when users see themselves as experts in charge of their privacy, or when they see worth in control independent of consequences. When users engage with Facebook because they appreciate the autonomy afforded by manipulating various privacy settings, they are mobilising industrial worth. However, when control is justified as avoidance of consequences (i.e. social) then forms of worth from another regime—such as repercussions or image management from the regime of *fame*—are mobilised for legitimising argumentations.

In the regime of *fame*, worth is derived from the reality of public opinion. Legitimacy comes only in the form of social status, visibility and celebrity. Attention-getting and being recognised are valued ends unto themselves and require the deliberate revealing of secrets. Individuals constructing justifications in this regime are anchored in the management of

reputation, image and social repercussions. When users post personal photos to Instagram or Facebook in the hopes of accumulating 'likes', or of being seen or recognised, or of being held accountable, they mobilise the regime of *fame.* Conversely, when users withhold from posting photos or personal data on Facebook, out of fear for the social consequences or potential implications to their reputation, they again draw justification from within this regime.

In contrast to the legitimacy of fame, the *domestic* regime roots legitimacy in tradition, the home, and familial bonds. Here, worth is structured by position within the family hierarchy, as in father to son or parent to child. Legitimacy is also dependent upon one's position relative to the household, as either insider or outsider, family or stranger. In the *domestic* regime the giving up of secrets is considered betrayal, as legitimacy derives from protecting the integrity of the home and adhering to rules of etiquette and proper behaviour. Users often construct *domestic* justifications for privacy conceptions when they treat their data privacy as a protected domain into which one must first be invited. Such invitations only occur when users consider others to be trustworthy and discreet[2]. When criticising breaches of 'netiquette' such as trolling comments, unauthorised tagging in photos, or Facebook 'friend' requests from unknown individuals, users mobilise the sense of good manners and propriety that are *domestic* forms of worth.

Often in tension with the domestic regime, the *civic* regime is founded upon the pre-eminence of the collective. Where the domestic prioritises custom and the inviolability of the home, the *civic* renounces the particular in favour of the general will. Claims to legitimacy stand on common interests expressed through spokespersons or representatives and embodied in law and legislation. When supporting government oversight of data-mining practices or the congressional subpoena of Facebook CEO Mark Zuckerberg, for example, users construct *civic*

[2] Here 'others' includes both individual and collective entities, i.e. businesses, organisations.

justifications because they conceptualise data privacy as something to be regulated in service of the greater good. The same form of worth—common interest—is mobilised when ranking safety concerns above privacy, such as when users consent to state monitoring of internet activity in support of counter-terrorism efforts.

Commonly the target of *civic* justifications, worth in the *market* regime involves competition and transaction. Legitimacy is found in pursuit of desires, and specifically in the acts of negotiation, buying and selling. Justification rests in taking advantage of opportunities to benefit, to deal, and to do business. Users often express *market* legitimacy when conceptualising data privacy as having exchange value. They trade it as part of a deal when consenting to cookie-tracking in order to gain access to websites, or when providing personal information to complete e-commerce transactions. Specific to social media platforms such as Facebook and Twitter, users mobilise *market* legitimacy when they express a recognition that they do business with these companies by exchanging personal data rather than currency for platform use.

Last of the initial six, the *inspired* regime is unique. Within this regime, legitimacy is derived from the immeasurable. Fundamental forms of worth within this regime are authenticity and uniqueness. Argumentations that mobilise forms of worth external to the individual (i.e. social, collective worths) are rejected in favour of privileging the particular. Value is found in the spontaneity expressed through creation and intuition, emotions and feelings. Inspired justifications of data privacy conceptualisations are often mobilised to keep intact that which makes one unique and distinct—to protect identity from outside influences. Examples of such argumentations criticise social media for encouraging inauthenticity, most often concerning presentations of a ‘curated’ self; a vanity considered superficial, false, and disconnected from one’s identity.

Finally, the seventh regime is the *network* regime. Eight years after the publication of the initial six, a new justificatory regime was established to fill in the descriptive gaps left when applying the existing regimes to a world increasingly organised by networks (Boltanski & Chiapello, 2005). The fundamental principle in this new regime is the notion of interconnected, ceaseless activity. Individuals find legitimacy in the flexibility and adaptability required by constant connectedness. In this regime, the world’s natural order is that of a network, one built upon computers and information technologies. This natural order is infrastructural to the contemporary data environment—there is no concept of data privacy without it. As such, users rarely mobilise it directly, and the assumption of its legitimacy serves as the foundation upon which all other justifications are then built. In the few instances when network forms of worth are drawn upon for legitimacy, it is invariably only to make explicit this assumption of a natural, network order.

These regimes provide a pluralistic framework for the exploration of the norm-sensitive contexts within which data privacy argumentation occurs. Each regime provides a filtered view of legitimacy and rejects any other categorisation, offering only its own “specific ordering” of the world (Boltanski & Chiappello, 2005, p. 167). Use of these regimes, therefore, represents a unique approach to the empirical categorisation of complex contextual phenomena, as well as changing norms. Argumentation styles and their related justifications open up to analysis the specific constructions of legitimacy and perceptions of appropriateness governing information flows; they reveal how different individuals, in different contexts, perceive context-integrity, as well as the relevant norms that preserve it and validate transgressions. Such contextually rich empirical categorisation offers significant opportunities for enriching data privacy study practices beyond traditional measures.

Traditional studies analysing survey responses on trust, risk, brand familiarity or platform knowledge (Gerber et al., 2018; Norberg et al., 2007) suffer from measuring externally-directed indicators. These indicated levels of trust or risk only capture perceptions of an 'other'—a company, a government, a platform or brand—and neglect the contexts and individual conceptualisations within which those perceptions are created or expressed. Through the resolution process of analytically applying regimes of justification within a context-integrity framework, this research attempts to unravel superficial perceptions of paradox and enhance a general understanding of contextual patterns influencing data privacy conceptualisations.

Methods & Data

The data for this study were collected from participants in both the United States of America and the Netherlands. Both countries are representative of Western liberal societies with high levels of internet usage and social media engagement (Appendix 1: graphs of usage), however, their regulatory contexts are dissimilar. American data privacy discourse and policy has historically been dominated by corporate actors[3], while the European discourse (for which the Netherlands serves as a proxy) has recently become dominated by both state and supranational regulatory perspectives (e.g. the Dutch Data Protection Act in 2016 and the EU GDPR [AVG] in 2018). This discrepancy between the two data privacy regulatory contexts allows a comparative analysis of how justifications differ across established contextual lines.

Sampling

While American participants were reached in various cities across the country via internet communication platforms (FaceTime, Skype), Dutch participants were interviewed in person in the cities of Rotterdam and Amsterdam. In total, 20 individuals were interviewed, ranging from

[3] This is shifting. Leading up to the 2020 election, data privacy has begun to figure prominently on the agendas of Democratic Party candidates eager to gain support by confronting Silicon Valley (Tolan, 2019).

21 to 73 years of age, equally divided between men and women, engaged in various occupations (Fig. 1). Age and gender provide two additional opportunities for comparative cross-context analyses.

Figure 1. Participant Overview*

Name	Age	Ethnicity	Occupation
Alex (M)	22	American	Engineering Graduate Student
Anne (F)	27	Dutch	Social Worker
Anouk (F)	24	Dutch	Psychology Student/Entrepreneur
Ashley (F)	60	American	Community Volunteer
Austin (M)	73	American	Retired Entrepreneur
Daniel (M)	34	African American	Attorney
Emily (F)	33	Asian-American	Nurse
Fleur (F)	25	Dutch	Social Sciences Graduate Student
Gijs (M)	41	Dutch Moluccan	Municipal Office Worker
Hannah (F)	25	American	Product Development and Marketing
Jacob (M)	23	American	Government Analyst
Jeroen (M)	59	Dutch	Actor/Self-Employed
Lars (M)	32	Dutch	Social Sciences Graduate Student
Lisa (F)	29	Dutch	Mental Health Worker
Matt (M)	61	American	Retired Engineer/Product Development Consultant
Mike (M)	36	American	Bank Investment Advisor
Sanne (F)	61	Dutch	Actress
Sarah (F)	34	American	Government Analyst
Stefan (M)	64	Dutch	Youth Protection Worker
Tessa (F)	21	Dutch	Music Instructor

Participant names have been altered for privacy considerations.

The sampling process occurred in two parts. First, interested individuals were sought out through friends, family, and fellow students via convenience and snowball sampling. Following the identification of potential participants, the second part employed a generic and purposive approach (Bryman, 2016, p. 412). This approach focused on identifying an ‘individual user’ collective, corresponding to earlier theorising that recognition of contextual influences on these actors is most often absent from discussions regarding data privacy policy. This user base is best represented by persons regularly engaging and participating in general online activities (e.g. blogging, purchasing, browsing, posting in social media), yet lacking increased technical sophistication (e.g. advanced coding skills, knowledge of programming languages) or extensive professional experience (e.g. algorithm writing, software development, big data analysis, dataveillance). Conversely, this base is ill-represented by those whose positions or occupations could be considered elements of technological “monopolies of knowledge” (Innis, 1951, p. 179-180) such as “developers” or other classes participating in privileged data privacy discourses, specifically those falling into the categories of the two most dominant actors: the state and technology corporations. Therefore, based on responses to the Pre-Interview Questionnaire (Appendix 2), excluded from the participant pool were any individuals with specific professional backgrounds in high technology, such as coders/programmers, software developers; those working in technical positions in fields such as cybersecurity and artificial intelligence; and those with positions of regulatory influence, working in relevant government or policy-making professions[4].

[4] These individuals are not irrelevant to the exploration of DP contexts, perceptions of agency, or discourses on data protection responsibilities; rather quite the opposite. However, the complexities surrounding privileged discourse participants render an exploration of justificatory regimes among "tech" workers and corporations outside both the current capability and scope of this particular study.

Data Collection & Interview Design: Context-Integrity Framework + Tests of Worth

Semi-structured interviews were conducted, exploring the various user argumentations surrounding data privacy concerns and responsibilities. Interviews lasted between 60-90 minutes in length, all interviews were recorded and transcribed in English, and positive control of all data was maintained following procedures outlined in the approved Ethics and Privacy Checklist (Appendix 3).

Figure. 2: Interview Phase Design

Each interview occurred in three phases and accomplished the two functions discussed earlier as constituting the process of 'Resolution' (Fig. 2). First, incorporating the context-integrity framework, the interview design addressed each of the four parameters—*contexts*, *actors*, *attributes*, and *transmission principles*—multiple times, from multiple angles. In this way, relevant participant contexts were fleshed out beyond the prevailing reductionism of balancing trust and risk levels, exposing the breadth of contextual considerations employed in constructing data privacy attitudes and managing disclosures. Second, each interview functioned as what Boltanski and Chiapello (2005) refer to as a *paradigmatic test* (p. 168). These tests serve to reveal the 'worth' or legitimacy of justifications within each regime by allowing an "appeal to the higher common principle" to stabilise competing claims (Boltanski & Thévenot, 2006, p. 138). By destabilising conceptualisations, the test provided participants the opportunity to

construct justifications and argumentations for themselves in real time, which would later be analysed to consolidate those regimes users perceived to be most legitimate for assigning worth.

Each interview began anchored in three open-ended questions: *what does it mean to you for something to be private, how do you define a violation of privacy, what is data privacy to you?* This first phase afforded participants opportunities to discuss a topic they may occasionally have given direct thought to, meaning their responses were direct exposures of contextual influences, actively constructed from their concerns and attitudes towards data privacy at the moment and not post hoc to survey completion. These constructs would later be coded into patterns and themes, then consolidated within different regimes of justification.

The second part of each interview consisted of a survey walkthrough. Eight questions (not including sub-bullets) were taken verbatim from the Pew Research Center Data Privacy Survey of 2014; however, participants were asked to go beyond the provided Likert-scale responses and expound upon their answers with supporting justifications. These questions also served to incorporate the various parameters of Nissenbaum's context-integrity framework, allowing a multifaceted exploration of data privacy conceptions, rather than limited bipolar assessments of opinions toward brand identity or security setting options. As a result of this design, participant responses demonstrate the versatility of the justification process, employing a plurality of regimes in their efforts to both establish legitimacy to their arguments or to delegitimize contradictory arguments.

The closing phase of the interview narrowed in on participants' specific conceptions of responsibility for data privacy and the justifications from which they derived, centred around three questions: *what does it mean to you for someone to be responsible for data privacy*; *according to you, who is responsible for data privacy*; *what does that responsibility entail*. Much

like the opening phase, this section afforded participants chances to discuss an even more uncommon topic, driving tailored argumentations to the presented test. These constructs would also later be coded into patterns and themes to be consolidated within different regimes of justification.

Data Analysis: Regimes of Justification

All data have been coded via a two-step coding process modelled on the process used in Arts et al. (2017). Each participant response was first coded inductively into a data matrix, identifying patterns and themes, iteratively refined as additional interviews were completed. In the second step, a deductive approach applied the seven justificatory regimes to sort the resulting codes, identifying those that could be constituted into coherent argumentation, critique, or compromise within particular regimes. Following this consolidation, the data were sorted by nationality, age, and gender to identify cross-contextual patterns of justification.

Results

The analysis of user constructed argumentations revealed coherent, measurable, and predictable patterns of contextual influence present within data privacy conceptualisations. While these constructed justifications varied between individuals—no two participants pulled from the same combination of regimes—there were patterns of regime mobilisation that occurred far more (or less) often than others. These patterns of mobilisation are presented in three parts.

The first part highlights those patterns of argumentation mobilised in personal or ‘ideal’ conceptions of privacy. These patterns are contrasted in the second part presenting how argumentation patterns changed when confronted with the ‘reality’ of data privacy responsibility and competing regimes. The final part presents a comparative look at the different argumentation

patterns found between Dutch and American participants, as well as those found between participants of different ages[5].

Conceptualising Data Privacy*:* The Ideal

Given *carte blanche* in conceptualising their 'ideal' notions of data privacy, users most commonly sought legitimacy by mobilising forms of worth from three of the seven regimes: the *domestic*, *fame*, and *industrial*[6].

Domestic

The *domestic* form of worth most often mobilised was the notion of privacy as a protected domain, requiring active discrimination of *inside* from *outside*. For many users, legitimacy surrounding data privacy stemmed from their perceptions of delineating domains, distinguishing insiders from outsiders, and exercising control over the integrity of their 'household'.

> "Privacy is maybe like creating your own space where you can put your stuff that's only for you, or only for you in relationship with maybe your wife or family."
> – Gijs (41, NL)

> "Private is my family life, the things my family says to me. And my family is very, very narrow. It's just, I think, my daughters and my partners."
> – Sanne (61, NL)

> "I think that the things that you share between family or friends, that's really important to someone; that you keep to yourself, that you keep in that little network."
> – Lisa (29, NL)

While often referring to their literal household or family, users also mobilised this notion of domain to compose harmonious spaces wherever legitimacy was gained by knowing whom to *include* and whom to *exclude*.

---

[5] Only age variations were found during analysis. A brief discussion of gender is included in the conclusion, as certain gender differences did arise but proved to be outside the analytical scope of this study.

[6] Again, the *network* regime is rarely independently referenced for legitimacy, but *all* participants underlined interconnectedness and regime objects (computers, information technologies) as infrastructural elements of the modern digital environment, within which other regimes were mobilised.

> “You would look at other people--you would compartmentalize and say well, there's some people that are friends and family that I would share a certain amount with them. And then there's the people that work for me in some capacity and that’s for another type of sharing. And then there's people that I well, need something from like doctors or whatever. And then that's a different type.”
>
> – Ashley (60, USA)

This exercise in moderating domains adds relational substance to traditional notions of access. It illuminates a critical element of context management neglected by reductionist measures: *positional worth.* This concept of positional worth speaks to *why* access is granted (insider status), and in what way *why* may consistently be derived (domain integrity).

Critical to positional worth was the notion of insider status, and in making this distinction, users relied on the mobilisation of two additional forms of domestic worth. Each data privacy ‘household’ was governed by unique norms and an oft-unwritten sense of propriety (netiquette). Worthy individuals—those allowed *inside*—were those who (a) were deemed trustworthy, discreet, or loyal, because they (b) could be expected to adhere to these particular rules of etiquette and proper behaviour.

> “So with friends, I might want for them to have more information about me. But a stranger maybe not so much…it has to do with trust. Trusting that the people who are privy to something about me will treat it in a way that I find appropriate. So I would expect a friend to not speak poorly of me or use information to sully my character. Whereas with a stranger, I might not know what they would do with whatever information I let them know.”
>
> – Sarah (34, USA)

These traits not only described how users perceived others, but they also characterised how users considered themselves and their own behaviours regarding privacy.

> “I'm also an alderman in our church so I have many pastoral discussions with people, so trust, keeping trust is really basic in my work, and also as an alder in our church. The most basic point for me: as my character, it's not very difficult to keep the privacy. Some people, they are very loose in it, I'm very strict. For me, the most poignant point is what do I communicate with my wife or not? If an intimate relationship, I like to discuss everything, and at the same time, I have to think the same questions, ‘Why do I bother her with that?’ Or ‘Why do I talk with her about people in our congregation?’”
>
> – Stefan (64, NL)

> "In my own home. I have a wife and three girls, three daughters, but I need my own privacy right? I don't want to expose the wrong things to the girls right?"
>
> – Mike (36, USA)

Participants were also keen to identify when their rules of etiquette and the integrity of their domain had been breached.

> "If you want to be an exhibitionist, that's fine…you think 'I have nothing to hide,' but you offend your neighbor because he thinks 'you're coming into my space.'"
>
> – Gijs (41, NL)

> "I used to work at an Italian restaurant and then it closed down. And a few months or years later, there was a drug lab. And then someone just posted to my mom, "Hey, isn't this the restaurant that your daughter used to work at?" That's a shitty story with the whole synthetic drug lab that I never knew anything about. I'm like, "Is it necessary?" And I responded. I was like, "Okay, don't you think this is a little weird to post?"
>
> – Tessa (21, NL)

> "The whole suggested friend thing that I also think is so weird because I got the first suggested friend thing from Facebook three months ago and then I get a lot of people who want to follow you, and I'm like, "I don't know you." And I always say, "No," no to that…I don't really post personal stuff but still, I don't want people that I really don't know to follow me."
>
> – Fleur (25, NL)

Breaches associated with concerns for data privacy—such as being Googled by strangers, unknowingly being 'tagged' in photos, or being contacted via social media by unknown persons—were most often associated with forms of worth from within the regime of *fame*.

Fame

The regime of *fame* is often at odds with the *domestic*. At the heart of this regime is the importance of public opinion and the desire for visibility. Etiquette and propriety are discarded, and the doors of the domestic household are flung open. The legitimacy derived from reputation or social esteem and the attention-seeking that requires the revealing of secrets is firmly rejected by the domestic for their potential to lead to betrayal.

> "When it comes to my family, I would never say things to accomplish other things, to use their things, their information to get something done with other people."

– Sanne (61, NL)

> "The violation, I think, occurs when you jump from unintended…to the unwanted, which is pretty much somebody telling your secrets."

– Daniel (33, USA)

Not all participants rejected these *fame* forms of worth. For some, public opinion and the value of recognition served several purposes. For Jeroen, a prominent Dutch actor through the 1990s, being recognised was essential to his professional success:

> "As an actor, if you want to have some success, you work hard to be a household name…And if you are a household name, you lose your privacy. But if you want to be successful, you have to lose your privacy on purpose. You have to be recognized on the street because if you are recognized on the street, that means that you have an audience."

– Jeroen (59, NL)

Others weighed the importance of privacy against the accountability offered through recognition and visibility.

> "Cyber accountability, where people are checking out your development and checking out what you're doing… it may be inspirational to someone to say, "I have 500 followers or whatever and let me push myself to an achievement or try to be a good example…people have tons of followers, like 500,000 followers. In that regard, I think it's a good thing because they are able to impact and influence and try to be their best self because they know a million people are watching you.

– Mike (36, USA)

> "Nowadays with social media, there's a new tier of friends, in the general sense of--you still have your close friends, just your friends--and now you have the social media friends, people that you rarely interact with. And so, people that use social media have a larger populace that they can affect, or they are hearing from."

– Alex (21, USA)

> "I was in a sorority in college, very typical. And when you'd go out on a weekend--I mean, everyone takes pictures, you post it on your Instagram, you post it on your Facebook. And there was a dedicated person in our sorority who would go and comment C-C for 'crooked crown' because your crown's a little crooked in this photo and you need to take it down…holding you accountable."

– Hannah (25, USA)

For these users, visibility seemed an inescapable reality of modern social life. It could be fought, to gain a little privacy, or it could be mobilised for greater benefits, such as influence, accountability, motivation, and even literal fame.

Shared by every mobilisation of the regime of *fame*—in both legitimising and delegitimising argumentations—were concerns for reputation and repercussions. Where domestic legitimacy is intrinsically underpinned by notions of shame and honour regarding one's family or household, legitimacy in the regime of *fame* is inseparable from one's *public image*.

> "The loss of social capital. Alienation from certain circles of colleagues, cohorts, people that I work with in the community."
>
> – Mike (36, USA)

> "They think the worst thing [is] 'my social status will be totally ruined' and they will be so bullied if it will get out."
>
> – Anouk (24, NL)

Users recognised the fundamental relationship between reputation and repercussions, and the different measures they took to manage data privacy or exert control over information mobilised these forms of worth.

> "And the reason I keep those separate and keep things private is because the way that people think of me may be influenced by these private things that I might not necessarily want to be the way that somebody thinks of me. I think privacy will always be relevant because at the end of the day people are always going to have perceptions of you."
>
> – Jacob (23, USA)

> "I can be honest and say I've kind of had a chip on my shoulder about whether or not people perceive me as intelligent. And I think people are predisposed to doing so in a business element and environment more so than they are in casual circumstances…When I wrote that legal article, I wanted to be taken seriously and so I did lock up my Twitter for a little bit. Because--I wouldn't even say it's protection of business consequences--I could care less if people want me to be their attorney or if my bosses want me to stick around. It is more the social aspect of it."
>
> – Daniel (33, USA)

An important distinction must be made here regarding the notion of control. In this instance, control derives legitimacy from its relation to forms of worth from the regime of fame,

specifically, the management of image and social consequences. This observation is essential because, within justificatory regime theory, control is predominantly understood as a form of worth from the *industrial* regime; in fact, it was the most mobilised form of industrial worth present in user data privacy argumentations.

Industrial

The legitimacy of control in the *industrial* regime is not rooted in *specific* consequences but is instead rooted in a *general notion* of consequence. Control in this regime is valued for its relation to predictable futures. Legitimacy in this regime is not derived from whether or not the consequences resulting from control are beneficial. Legitimacy is established simply by the existence of a relationship of control that effects consequences, positively or negatively.

This may seem semantic, but it constitutes a noticeable difference in how users mobilised the value of control. In the regime of fame, for example, control was valued for the resulting social consequences, such as gaining esteem or avoiding stigma and preserving reputation.

> "I want to maintain that control of what people think of me." – Jacob (23, USA)

> "When we all graduated…you immediately put your profile on private, you could immediately change your name, control all your things. Because now, it's time to job search and they can't find those pictures of you with the red solo cup."
>
> – Hannah (25, USA)

When mobilising the *industrial* regime, however, users sought legitimacy in control based solely on the inherent worth of autonomy.

> "Privacy is power for you to take care of yourself…for you to control the narrative."
>
> – Emily (34, USA)

> "I put myself out there confidently because I'm curating and decide what I put out there. The moment somebody else makes that decision for me and makes it public, I get really sad I think"
>
> – Hannah (25, USA)

> "Because I didn't say yes."

– Anouk (24, NL)

A related negative example came from Lars, wherein he acknowledged the industrial worth of control, but rejected it in favour of another industrial form of worth, efficiency:

> "And if I wanted to use all the methods to keep my data private, then I would have to go out and figure out how that works--I don't know. It is just a lot of hassle…Yeah. It's fine the way it is."
>
> – Lars (32, NL)

This relational notion of control has significant consequences for the study of privacy. Within the privacy paradox, users are portrayed as inconsistent in their data privacy attitudes and behaviours. This results from traditional approaches that reduce notions of control or access to one-dimensional indicators: does the user control the data or do they not. The value of using justificatory regimes as analytical constructs lies in their capacity to go beyond reductionism and expose relational notions like control (and access). Through this exposure, the empirical categorisation of data privacy contexts becomes possible.

Navigating Responsibility and Competition: The Real

Tests

In the modern digital environment, however, users are rarely (if ever) given the opportunity to rely on their ideal conceptualisations of data privacy for justification. More often than not, users are confronted with the data privacy reality of having to construct coherent argumentations from conflicting norms and competing regimes. In the language of regime theory, they are confronted with *paradigmatic tests*. One such test example was shared by Lars, about a dilemma he and his wife faced regarding Facebook and pictures of their new-born son:

> "In the fourth week, I think, we had this post on Facebook. Me and my wife, we actually really debated about it like, "Should we put this online, or should we put him online?" He has nothing to say about what we put out there, right? There's a chance that those pictures

> might still be there when he's 20 years old. Does he want that? What would he say about that? But also--because he has no control over what we do, right? But then again, we also wanted to share with Facebook because somehow that's that important, that everybody knows.”

In this test, two forms of worth from separate regimes compete for legitimacy. Initially, Lars considers mobilising the legitimacy of control (*industrial*) when he and his wife expressed concern that their son had “nothing to say” over what would be posted of him during his infancy. The value they placed on autonomy was then pitted against the value of visibility and recognition (*fame*). For Lars and his wife, it was also important that they reveal this aspect of their lives and share with their social circles. Ultimately, they would decide to share: “So, in the end--and I swear it took us a week to contemplate this and come up with something that we could both agree on. But we added one picture. It was okay.” However, these two mobilisations were not the only potentially relevant options.

Justificatory regimes are a pluralistic framework, and any test can potentially involve any number of relevant regimes. For Lars’ test, as an example, there could have been domestic mobilisation. Within the domestic regime, parents sit at the head of the household; therefore, whatever their decision, its legitimacy would be inherent to their superior position in the familial hierarchy. However, if there were a family tradition of being discreet and reserved, the decision to post might be considered an illegitimate breach of etiquette or custom. This *pluralism* is essential because it supports the exposure of contextual influences. Through the regime framework, it is possible to identify and categorise the complex contextual influences on both Lars’ conceptualisation of data privacy (industrial & fame) and his relevant behaviours (fame).

While these kinds of organic tests appeared several of times during the interviews, the interviews were themselves designed as tests, hinging on the concept of *responsibility*.

Who is Responsible?

Because responsibility flows *to* one thing *from* another, responsibility is a relational notion, much in the same way that access and control are. The critical difference for this study was that control and access were familiar topics—established in user data privacy discourse—while responsibility was an unfamiliar notion reserved for the privileged discourses from which users were historically excluded. Following open-ended discussions of (ideal) conceptualisations of data privacy, users were asked to again construct justifications in real time by identifying “who is responsible for data privacy”. Users thus encountered a unique test, destabilising their immediate data privacy conceptualisations. In such cases of instability, regime theory posited that two standard styles of argumentation would anchor individual efforts, leaving individuals feeling less uncertain and more stable in their justifications. These were the argumentation styles of *compromise* and *critique*.

Compromise & Critique

In resolving their Facebook dilemma, Lars and his wife had engaged in an example of compromise. Rather than completely delegitimise the industrial worth of control, they chose to compromise with the regime of fame, posting only one photo of their son and minimising the amount of digital exposure over which he lacked control. Critiques, on the other hand, seek the legitimacy of one regime over another. For example, the few mobilisations of the *inspired* regime were invariably critiques of fame, delegitimising visibility and public opinion as inauthentic and disingenuous.

> “I'll get a lot of people that say happy birthday and this and that and--there's a whole bunch of them--and I’ve got a hundred to respond to. If I don't put any [birthdate on

> social media] then I know maybe a dozen people who know me really well, who know my birthday, will say happy birthday to me; in which case, I'll respond. But I don't want a thousand people who don't really care about me or whatever but want to send happy birthday because they want to sell something to me.”
>
> – Matt (61, USA)

> “I always think they want to show the world an image of themselves--maybe they're insecure and want to feel better, or want to show like, ‘oh look at me having a perfect great life’, and because--if I look at my own life--I don't put a lot of that on the internet…for me also the digital world is not the real world. And what we now have is real interaction, and all those fast chats and reactions you get on your social media, that's all nice. But everybody can do that.”
>
> – Fleur (25, NL)

In navigating the responsibility test, users demonstrated two curious shifts in regime mobilisation patterns. First, though their ideal conceptualisations were dominated by three of the seven regimes, of those three, only the *industrial* regime was mobilised around responsibility, and this occurred alongside a significant increase in mobilised forms of worth from the *civic* and *market* regimes. The second curious shift was that this pattern was ubiquitous. Although user conceptualisations did demonstrate some contextual variation (discussed in subsequent sections) when conceptualising around data privacy responsibility, across age and nationality users overwhelmingly mobilised industrial, civic, and market forms of worth.

Via these mobilisations, users constructed a single, oppositional set of argumentations: a *civic-market compromise* supporting regulation, and an *industrial-civic critique* lamenting the inefficiencies of administrative processes.

The regulatory compromise sought to ease the competition between collective interests (safety) and general market incentives (profit).

> “I think ‘Yeah, maybe the state should intervene. Maybe the state should keep controls at some level over tech companies.’ But I'm also a free market guy, so it's like, ‘No. I don't want the state involved at all.’ So there is an interesting tension there between privacy, tech, and the state.”
>
> – Mike (36, USA)

The legitimacy of this compromise came from balancing the pursuit of profit and market growth, with collective oversight and governed rule, respecting both regulatory legislation and free markets.

> “I think that I would use a model that's been in place already in this context with the financial services industry, with the Securities and Exchange Commission…create a commission that oversees the issue of privacy. And then, the state would then provide oversight, and--But not too much. Right? I mean, because you don't want to stunt motivation.”
>
> – Mike (36, USA)

> “You don’t want the government being so controlling that you tie the hands of corporations and free enterprise. At the same time, we don’t want companies to run amok and do all kinds of crazy things so I mean, I think there has to be sensible government regulations.”
>
> – Ashley (60, USA)

> “So the playing field is made by the government. And so the responsibility of the company is to play within the playing field that's set up by legislation.”
>
> – Jeroen (59, NL)

Users also recognised the difficult realities such a compromise faced. Captured in their critique of administrative inefficiencies, users delegitimised civic worths in light of a world they considered dominated by the demands of efficiency and function.

> “With regulatory issues, you would have to be specific in your verbiage and that's a headache. And I don't think the government is interested in finding specific verbiage to protect privacy…I think it's asking a lot to say that the government will pass a bill that will be worded correctly and timelessly. Like a bill that doesn't have to evolve every six months because internet algorithms or users or marketers have found a way to loophole in that bill.”
>
> – Emily (33, USA)

> “Technology goes faster than--yeah, than the human rights book is being written. And there are so many laws that should be there, but they aren't there because it's much more complicated to make a law than to make a website.”
>
> – Anouk (24, NL)

> “You sign up for Facebook and you have a 30 page, 30,000 word document to read about stuff like that. That needs to be streamlined, that needs to be easier.”
>
> – Mike (36, USA)

Such cross-contextual similarity in argumentation highlights a critical benefit of regime analysis relative to context-integrity: the capacity to render contextual influences *measurable* and *predictable*. When freely conceptualising data privacy, the breadth of mobilised forms of worth was wide, as forms of worth from each regime were mobilised at least once, supporting the theoretical notion of plurality: any test may mobilise any number of regimes at any time. However, while supported in *individual* tests, this plurality of available regimes does not hold for tests in *aggregate*. Supporting evidence is that, though no two users mobilised the same combination of regimes, certain regimes were mobilised more often across the collective conceptualisation of data privacy. Further evidence lies in the significant cross-context similarities in argumentations constructed concerning data privacy responsibility. Not only were *different* regimes mobilised in confronting the test than were mobilised in conceptualising data privacy, but they were *the same* regimes, constructed along *the same* lines of interaction across the different contexts of nationality, age and gender.

It is, therefore, reasonable to assess that issues, tests, or populations—when analysed in aggregate—have parameters limiting the plurality of available relevant regimes. Such parameters are completely in line with context-integrity notions of “context-relative informational-norms” governing the appropriateness of information flow. Once identified, as a result of regime analysis, these norms—the complex *whys* behind contextual influence—become measurable and even predictable, given an appropriately aggregate data set.

Contextualising Mobilisation Pattern Variations

In addition to striking cross-context similarities, there were some notable variations found across divisions of age and nationality. Further examining data privacy conceptualisations, the following section provides a synopsis of contextual variations in regime mobilisation patterns.

Age

Concerning age, the most notable variation arose between the youngest and oldest participants. Among older participants, those aged 45 and over, forms of worth from within the *domestic* regime dominated their ‘idea’ conceptualisations. Among younger participants, aged 25 and under, the forms of worth they most mobilised originated in the regime of *fame*. This variation follows quite well from regime theory.

Older participants, having tradition and experience behind them, are also more likely to be higher in household hierarchies, either as parents, grandparents, supervisors or directors. They therefore logically afford more legitimacy to forms of worth from the *domestic* regime wherein they are inherently afforded pride of place. The young, however, are lower on familial hierarchies and have access to much less legitimacy within the domestic regime. Left to seek legitimacy elsewhere and having come of age in an era defined by the interconnectedness of social media, younger participants are understandably comfortable in the regime of *fame*. Legitimacy rooted in public opinion and visibility is not only structurally in their favour, via social networking culture, but fame and public esteem in western cultures have historically favoured youth. The result is that both groups construct justifications directly excluding the other and rejecting their claims to legitimacy.

Nationality

While some notable differences presented themselves between Dutch and American participants, their patterns of mobilisation were far more similar than dissimilar. Both groups favoured civic and industrial regimes in their mobilisations surrounding responsibility for data privacy, and both were critical of forms of worth legitimised in the regime of fame. The differences between the

two groups arose within their mobilisations of personal data privacy conceptualisations and in their common critiques and compromises.

Dutch personal conceptualisations of data privacy relied heavily on domestic legitimacy, specifically domain forms of worth. Dutch participants were also more likely to compromise with the civic regime and were more critical of the regime of fame. In their constructed justifications, American users expressed predominantly industrial mobilisations, heavily rooted in the worth of control. Americans also constructed compromises most often with market forms of worth and were most critical of legitimacies derived from the civic regime. These variations run nearly parallel to established cultural differences. Most specifically, that the Dutch would find compromise easier within the civic regime is in line with the Dutch preference for Social Democracy and an expectation of state interference and regulation in social affairs. Especially in light of the data privacy focus, Dutch civic compromise finds an exemplary expression in the Dutch Data Protection Act and EU GDPR (AVG). That the Americans would be more critical of civic forms of worth and more amenable to compromises with market legitimacies echoes long-standing American scepticism of government involvement in social affairs, a preference for free markets, and a hesitancy to adopt broad data privacy regulation, preferring to let the corporate sector police itself.

Conclusion & Discussion

The exploration of complex contextual influences involved in user data privacy conceptualisations unearthed two specific advantages to using an integrated regime analysis framework over traditional reductionist approaches. First, contextual influences tied to the relational notions of positional worth, control and access can be consistently identified and categorised, no longer needing to be omitted in measurement. Second, via paradigmatic tests,

complex norm interactions can be exposed and measured in the forms of compromises and critiques. These advantages, taken together, facilitate a context-rich analysis that is coherent, measurable and predictable.

Capitalising on these advantages, an analysis of consistent patterns of contextual influence within user conceptualisations resolves the privacy paradox and enhances understanding of user-norm relationships regarding data privacy. Justifications constructed by Dutch and American users demonstrate that contextual influences can be coherent, measurable, and predictable across contexts, surpassing the limitations of traditional reductionist measures that fail to reconcile user attitudes and behaviours. This research contributes to a broad and evolving understanding of complex, norm-sensitive issues such as data privacy, which grow increasingly relevant as technological and corporate interest in privacy norms steadily increases.

Gender

A brief note regarding gender before discussing limitations and implications. There were no significant gender differences found relating to regime analysis or mobilisation patterns. However, when discussing data privacy violations, male and female participants differed very specifically on one point. Female participants expressed concern or experience of violation in the first person–I, me, my–while men rarely expressed experiencing violation at all, and more often inserted daughters, wives, teen girls or women in general into the subject position when conveying concerns. Though outside the scope of this study, it poses significant questions regarding the relationship of privacy violation to gender identity.

Limitations & Implications

No research is undertaken without limitations; however, limitations may offer avenues for additional research.

While the justificatory framework seems very effective at categorisation, there may be an inherent “relative blindness” (Jagd, 2011) toward forms of justification that fail to fit established regimes. In this study, the concept of ‘safety’ in data privacy proved challenging to code for this reason. There is significant ambiguity around the idea of safety: in argumentations around data privacy, references to safety abound but fail to clearly originate in any single regime, leading to inconsistency. For this study, because safety was such a prominent reference of worth, and because it was so often presented during discussions of common interests (*civic*) and control (*industrial*), it is categorised as a form of compromise between these two regimes.

Additionally, the sample size used for this study is small ($n = 20$), in comparison to the broader digital user base represented, and potentially suffers from an over-representation of conservative ideologies based on the communities from which participants were drawn. The use of only a single coder and the subjective establishment of a collective user identity also pose potential questions of validity.

One opportunity to address the above limitations and build upon the results of this research lies in extending this design to incorporate additional collective actors, especially those involved in privileged data privacy discourses (corporate & state). By increasing the data set, and employing multiple coders, researchers can capitalise on the advantages of regime analysis. Potential also exists for a regime- or mobilisation pattern-based survey tool, allowing for larger data sets and faster analyses of a variety of complex, norm-sensitive issues.

Such opportunities, in light of both the ever-growing interest in norm-entrepreneurship and the speed of technologically driven social change, offer a wealth of opportunities for those interested in exploring the nature of regime and norm evolution or change, via the implementation of similarly integrated regime analysis and context-integrity frameworks.

References

Arts, I., Buijs, A. E., & Verschoor, G. (2017). Regimes of justification: competing arguments and the construction of legitimacy in Dutch nature conservation practices. *Journal of Environmental Planning and Management, 61*(5–6), 1070–1084. https://doi.org/10.1080/09640568.2017.1319346

Barber, G. (2019, May 14). Microsoft wants to protect your identity with bitcoin. *Wired.* Retrieved from https://www.wired.com/story/microsoft-wants-protect-identity-bitcoin/

Brandom, R. (2019, June 8). Apple’s new sign-in button is built for a post-Cambridge Analytica world. *The Verge.* Retrieved from https://www.theverge.com/2019/6/8/18656885/apple-single-sign-on-button-sso-google-facebook-cambridge-analytica-privacy

Bryman, A. (2016). *Social Research Methods 5th Ed.* Oxford: Oxford University Press

Boltanski, L., & Chiapello, E. (2005). The New Spirit of Capitalism. *International Journal of Politics, Culture, and Society, 18*(3-4), 161-188. doi: 10.1007/s10767-006-9006-9

Boltanski, L., & Thévenot, L. (2006). *On justification: Economies of worth*. Princeton, NJ: Princeton University Press

boyd, d., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society, 15*(5), 662-679. doi: 10.1080/1369118X.2012.678878

Carr, A. (2018, November 15). Silicon Valley doesn’t want the US to get too hasty about regulations. *Bloomberg News*. Retrieved from https://www.bloomberg.com/news/articles/2018-11-15/silicon-valley-doesn-t-want-the-u-s-to-get-hasty-on-regulations

Cyphers, B., Gebhart, G., & Schwartz, A. (2018, December 31). *Data privacy scandals and public policy picking up speed: 2018 in review*. Retrieved from https://www.eff.org/

deeplinks/2018/12/data-privacy-scandals-and-public-policy-picking-speed-2018-year-review

Forbes Technology Council. (2018, August 15). 15 Unexpected consequences of GDPR. *Forbes.* Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#72dbe67d94ad

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226-261. doi: 10.1016/j.cose.2018.04.002

Innis, H. (1951). *The bias of communication*. Toronto: University of Toronto Press

Introna, L. D. (2000). Workplace surveillance, privacy and distributive justice. *ACM SIGCAS Computers and Society, 30*(4), 33. https://doi.org/10.1145/572260.572267

Jagd, S. (2011). Pragmatic sociology and competing orders of worth in organizations. *European Journal of Social Theory, 14*(3), 343–359. doi: 10.1177/1368431011412349

Laskai, L. (2019, January 8). Year in review: The year of data protection. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/year-review-year-data-protection

Lemasson, G. (2015). On the legitimacy of cultural policies: analysing Québec’s cultural policy with the Economies of Worth. *International Journal of Cultural Policy, 23*(1), 68–88. https://doi.org/10.1080/10286632.2015.1035265

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051–1067. doi:10.1177/1461444814543995

Nippert-Eng, C. (2010). *Islands of privacy*. Chicago: Chicago University Press

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, California: Stanford University Press

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1), 100-126. doi: 10.1111/j.1745-6606.2006.00070.x

Rainie, L. (2018, March 27). Americans’ complicated feelings about social media in an era of privacy concerns. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Rand, D. (2019, February 26). The first unintended consequences of GDPR. Retrieved from https://www.hpe.com/us/en/insights/articles/the-first-unintended-consequences-of-gdpr-1902.html

Roberge, J., & Melançon, L. (2015). Being the King Kong of algorithmic culture is a tough job after all. *Convergence: The International Journal of Research into New Media Technologies, 23*(3), 306–324. https://doi.org/10.1177/1354856515592506

Silber, I. F. (2003). Pragmatic sociology as cultural sociology: Beyond repertoire theory? *European Journal of Social Theory, 6*(4), 427-449.

Singh, K. (2019, May 25). First American says product defect could have caused customer data exposure. *Reuters*. Retrieved from https://www.reuters.com/article/us-first-am-cyber/first-american-says-product-defect-could-have-caused-customer-data-exposure-idUSKCN1SV017

Smith, A. (2017). Americans and Cybersecurity. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Spillman, L. (2002). Introduction: Culture and cultural sociology. In L. Spillman (Ed.), *Cultural Sociology* (pp. 1-16). Malden, MA: Blackwell

Sunstein, C. R. (1996) Social norms and social roles. *Columbia Law Review, 96*, 903-968

Tolan, C. (2019, April 7). As Democratic candidates target big tech, “the honeymoon is over” for Silicon Valley. *The Mercury News*. Retrieved from https://www.mercurynews.com/2019/04/07/big-tech-democratic-presidential-race-2020-silicon-valley/

Tufekci, Z. (2017) Twitter and tear gas: The power and fragility of networked protest. Hanover, CT: Yale University Press

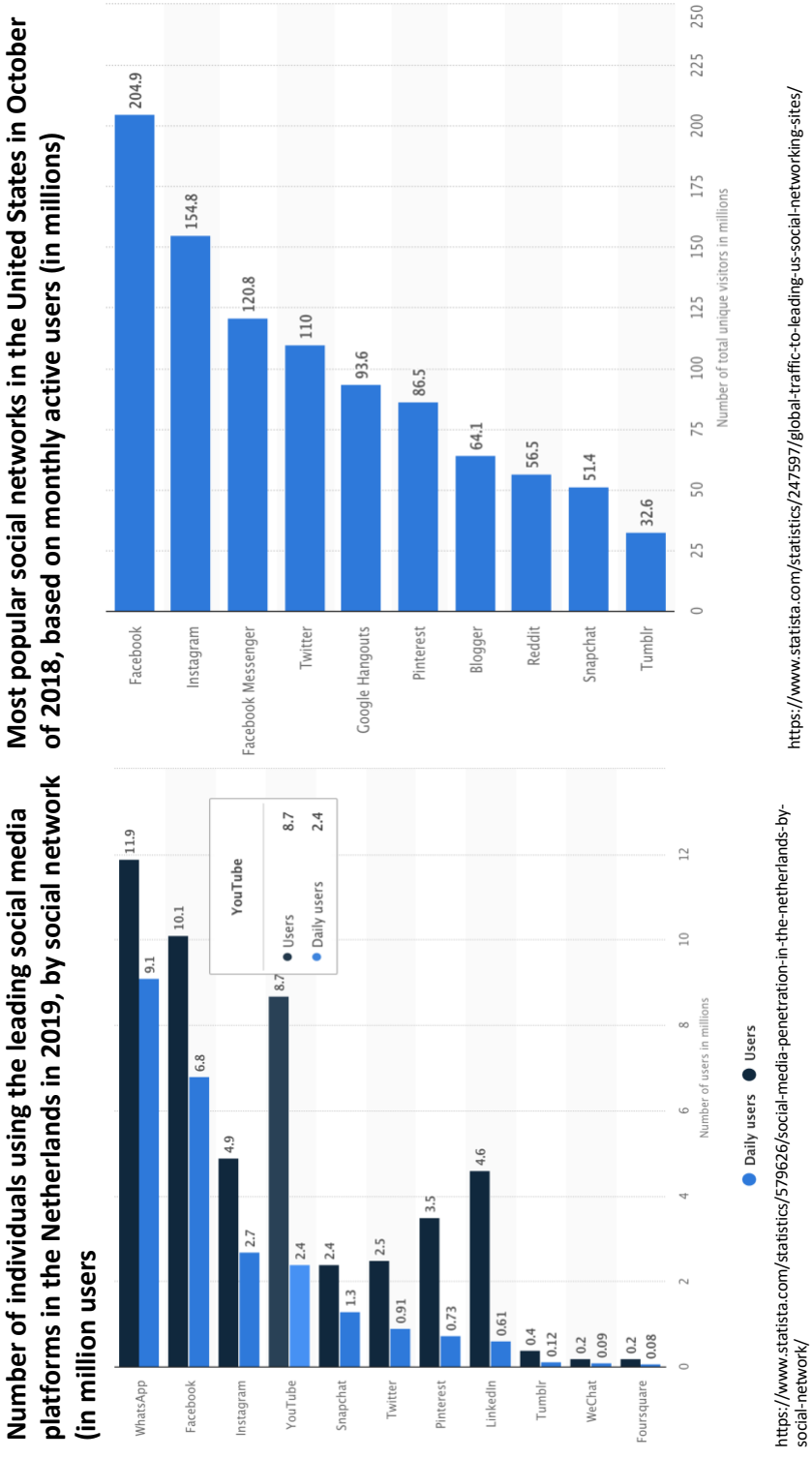
van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197-208.

Viveiros, B. N. (2018, December 12). Data privacy concerns on rise: Report. Retrieved from https://www.chiefmarketer.com/data-privacy-concerns-on-rise-report/

Wagner, P. (1999). After Justification: Repertoires of evaluation and the sociology of modernity. *European Journal of Social Theory*, *2*(3), 341–357.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT Privacy. *Proc. ACM Hum-Comput. Interact., 2*, CSCW, Article 200, 1-20. doi:10.1145/327

Appendix 1


Most popular social networks in the United States in October of 2018, based on monthly active users (in millions)
Facebook 204.9
Instagram 154.8
Facebook Messenger 120.8
Twitter 110
Google Hangouts 93.6
Pinterest 86.5
Blogger 64.1
Reddit 56.5
Snapchat 51.4
Tumblr 32.6
0 25 50 75 100 125 150 175 200 225 250
Number of total unique visitors in millions
https://www.statista.com/statistics/247597/global-traffic-to-leading-us-social-networking-sites/
Number of individuals using the leading social media platforms in the Netherlands in 2019, by social network (in million users
WhatsApp 11.9 9.1
Facebook 10.1 6.8
Instagram 4.9 2.7
YouTube 8.7 2.4
Snapchat 2.4 1.3
Twitter 2.5 0.91
Pinterest 3.5 0.73
LinkedIn 4.6 0.61
Tumblr 0.4 0.12
WeChat 0.2 0.09
Foursquare 0.2 0.08
YouTube Users 8.7 Daily users 2.4
0 2 4 6 8 10 12
Number of users in millions
Daily users Users
https://www.statista.com/statistics/579626/social-media-penetration-in-the-netherlands-by-social-network/

Appendix 2

PRE-INTERVIEW QUESTIONNAIRE (Pew Research Center Data Privacy Survey 2014)

Please include your answers to the following questions in your email, in the following format: Question/Answer "A/E, B/A, C/C, etc."

Would you consider yourself to have a ***professional background*** and/or ***more than average experience*** in any of the following: ***cybersecurity***, ***algorithm development*** (i.e. for 'big data' analytics or 'internet of things' operations or similar fields), ***data privacy regulation*** (i.e. through lobbying, legal action, policy creation, etc.)?
A) Yes
B) No

A) Overall, how often do you use the internet –
    A) Several times a day
    B) Once a day
    C) At least once a week
    D) Less often
    E) Refused

B) Do you access the internet on a cell phone, tablet or other mobile handheld device, at least occasionally?
    A) Yes
    B) No
    C) Refused

C) Do you own a cell phone? If so, is it a 'smartphone' (iPhone, Android, Blackberry or Windows phone)
    A) Yes; Yes
    B) Yes; No
    C) No
    D) Refused

D) Do you ever use online social networking sites like Facebook or Twitter?
    A) Yes
    B) No
    C) Refused

E) Do you ever use online purchasing platforms like Amazon or Bol.com?
    A) Yes
    B) No
    C) Refused

F) Are you familiar with online banking or financial investment services?
    A) Yes
    B) No
    C) Refused

G) Are you familiar with the existence of online dating platforms/applications such as E-Harmony, Match, Tinder?
    A) Yes
    B) No
    C) Refused

Appendix 3

ERASMUS UNIVERSITEIT ROTTERDAM

CHECKLIST ETHICAL AND PRIVACY ASPECTS OF RESEARCH

INSTRUCTION

This checklist should be completed for every research study that is conducted at the Department of Public Administration and Sociology (DPAS). This checklist should be completed *before* commencing with data collection or approaching participants. Students can complete this checklist with help of their supervisor.

This checklist is a mandatory part of the empirical master's thesis and has to be uploaded along with the research proposal.

The guideline for ethical aspects of research of the Dutch Sociological Association (NSV) can be found on their website (http://www.nsv-sociologie.nl/?page_id=17). If you have doubts about ethical or privacy aspects of your research study, discuss and resolve the matter with your EUR supervisor. If needed and if advised to do so by your supervisor, you can also consult Dr. Jennifer A. Holland, coordinator of the Sociology Master's Thesis program.

PART I: GENERAL INFORMATION

Project title: *Click "Accept": Exploring justification & responsibility in unraveling the 'privacy paradox'*

Name, email of student: Ryan Morgan, 508015rm@student.eur.nl

Name, email of supervisor: Julian Schaap, schaap@essb.eur.nl

Start date and duration: 30 January 2019, 7 months

Is the research study conducted within DPAS **YES** - NO

If 'NO': at or for what institute or organization will the study be conducted?
(e.g. internship organization)

PART II: TYPE OF RESEARCH STUDY

Please indicate the type of research study by circling the appropriate answer:

1. Research involving human participants. **YES** - NO

   If 'YES': does the study involve medical or physical research? YES - **NO**
   Research that falls under the Medical Research Involving Human Subjects Act (WMO) must first be submitted to an accredited medical research ethics committee or the Central Committee on Research Involving Human Subjects (CCMO).

2. Field observations without manipulations that will not involve identification of participants. YES - **NO**

3. Research involving completely anonymous data files (secondary data that has been anonymized by someone else). YES - **NO**

PART III: PARTICIPANTS
(Complete this section only if your study involves human participants)

Where will you collect your data?
—American participants will be contacted and interviewed online, while Dutch participants will be contacted and interviewed in-person in the cities of Rotterdam and Amsterdam.

Note: indicate for separate data sources.

What is the (anticipated) size of your sample?
—12-16 individuals

Note: indicate for separate data sources.

What is the size of the population from which you will sample?
—The population sizes for the respective samples are 290 million for the American set, and 15.88 million for the Dutch set (sizes reflect internet users as percentage of national populations).

Note: indicate for separate data sources.

1. Will information about the nature of the study and about what participants can expect during the study be withheld from them? YES - **NO**

2. Will any of the participants not be asked for verbal or written 'informed consent,' whereby they agree to participate in the study? YES - **NO**

3. Will information about the possibility to discontinue the participation at any time be withheld from participants? YES - **NO**

4. Will the study involve actively deceiving the participants? YES - **NO**
   Note: almost all research studies involve some kind of deception of participants. Try to think about what types of deception are ethical or non-ethical (e.g. purpose of the study

is not told, coercion is exerted on participants, giving participants the feeling that they harm other people by making certain decisions, etc.).

5. Does the study involve the risk of causing psychological stress or negative emotions beyond those normally encountered by participants? YES - **NO**

6. Will information be collected about special categories of data, as defined by the GDPR (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, data concerning mental or physical health, data concerning a person's sex life or sexual orientation)? **YES** - NO

7. Will the study involve the participation of minors (<18 years old) or other groups that cannot give consent? ~~**YES**~~ / NO

8. Is the health and/or safety of participants at risk during the study? YES - **NO**

9. Can participants be identified by the study results or can the confidentiality of the participants' identity not be ensured? YES - **NO**

10. Are there any other possible ethical issues with regard to this study? YES - **NO**

If you have answered 'YES' to any of the previous questions, please indicate below why this issue is unavoidable in this study.
In researching the 'regimes of justification' relevant to how users locate/assign responsibility for data protection, there is significant theoretical justification for potential differences between age cohorts, demonstrated by the work of Marwick & boyd (2014), as well as along cleavage lines such as race/ethnicity, politics, and religion. This is especially salient within the racialised political context of the United States.

What safeguards are taken to relieve possible adverse consequences of these issues (e.g., informing participants about the study afterwards, extra safety regulations, etc.).
All participants will be provided informed consent forms, ~~with parents or guardians being required to complete prior to the participation of a minor~~. Personally identifying data will not be maintained beyond generic demographic indicators, and any and all names used in the results will be changed and have their data anonymised.

Are there any unintended circumstances in the study that can cause harm or have negative (emotional) consequences to the participants? Indicate what possible circumstances this could be.
The only potential negative consequence or encounter could be the recounting of an upsetting experience of data privacy violation or identity theft; however, the questions put to participants are not designed to elicit any details around specific encounters of this kind.

Please attach your informed consent form in Appendix I, if applicable.

Part IV: Data storage and backup

Where and when will you store your data in the short term, after acquisition?
After collection, the data will be maintained in two independent, password protected external hard-drives, secured with my research supervisor and not linked to any cloud databasing architecture.
Note: indicate for separate data sources, for instance for paper-and pencil test data, and for digital data files.

Who is responsible for the immediate day-to-day management, storage and backup of the data arising from your research?
I will be the sole individual responsible for protecting and managing the storage and backup of any collected data.

How (frequently) will you back-up your research data for short-term data security?
Data on both the primary and secondary hard-drives will be backed up weekly and immediately following each interview.

In case of collecting personal data how will you anonymize the data?
—Personal data will be anonymised using random coding in conjunction with the data on the primary drive, separated form participant information on the secondary drive.
Note: It is advisable to keep directly identifying personal details separated from the rest of the data. Personal details are then replaced by a key/ code. Only the code is part of the database with data and the list of respondents/research subjects is kept separate.

PART VI: SIGNATURE

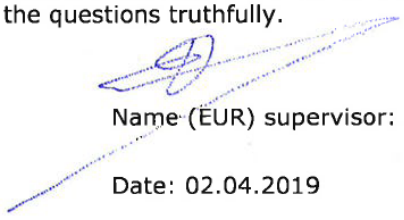
Please note that it is your responsibility to follow the ethical guidelines in the conduct of your study. This includes providing information to participants about the study and ensuring confidentiality in storage and use of personal data. Treat participants respectfully, be on time at appointments, call participants when they have signed up for your study and fulfill promises made to participants.

Furthermore, it is your responsibility that data are authentic, of high quality and properly stored. The principle is always that the supervisor (or strictly speaking the Erasmus University Rotterdam) remains owner of the data, and that the student should therefore hand over all data to the supervisor.

Hereby I declare that the study will be conducted in accordance with the ethical guidelines of the Department of Public Administration and Sociology at Erasmus University Rotterdam. I have answered the questions truthfully.

Name student: Ryan A. Morgan

Date: 02.04.2019



Name (EUR) supervisor: Julian Schaap

Date: 02.04.2019