When Do Data Collection and Use Become a Matter of Concern? A Cross-Cultural Comparison of U.S. and Dutch Privacy Attitudes

JESSICA VITAK[1]
University of Maryland, College Park, USA

YUTING LIAO
Intuit Inc., USA

ANOUK MOLS
DANIEL TROTTIER
Erasmus University Rotterdam, The Netherlands

MICHAEL ZIMMER
Marquette University, Wisconsin, USA

PRIYA C. KUMAR
The Pennsylvania State University, USA

JASON PRIDMORE
Erasmus University Rotterdam, The Netherlands

Around the world, people increasingly generate data through their everyday activities. Much of this happens unwittingly through sensors, cameras, and other surveillance tools on roads, in cities, and at the workplace. However, how individuals and governments think about privacy varies significantly around the world. In this article,

Jessica Vitak: jvitak@umd.edu
Yuting Liao: yliao598@terpmail.umd.edu
Anouk Mols: mols@eshcc.eur.nl
Daniel Trottier: trottier@eshcc.eur.nl
Michael Zimmer: michael.zimmer@marquette.edu
Priya C. Kumar: priya.kumar@psu.edu
Jason Pridmore: pridmore@eshcc.eur.nl
Date submitted: 2022-01-18

[1] The authors thank Katie Chamberlain Kritikos for her contributions to the project. This study was funded by National Science Foundation under Grant Nos. 1640640 and 1640697, and by the Netherlands Organization for Scientific Research under Grant No. 628.001.024.

we explore differences between people’s attitudes toward privacy and data collection practices in the United States and the Netherlands, two countries with very different regulatory approaches to governing consumer privacy. Through a factorial vignette survey deployed in the two countries, we identify specific contextual factors associated with concerns regarding how personal data are being used. Using Nissenbaum’s framework of privacy as contextual integrity to guide our analysis, we consider the role that five factors play in this assessment: actors (those using data), data type, amount of data collected, reported purpose of data use, and inferences drawn from the data. Findings indicate nationally bound differences as well as shared concerns and indicate future directions for cross-cultural privacy research.

Keywords: privacy, trust, contextual integrity, data collection, cross-cultural, General Data Protection Regulation

From posting on social media to tracking sleep with wearable devices, people increasingly generate data about themselves through their everyday activities. Much of this data collection happens unwittingly, thanks to sensors, cameras, and other surveillance tools on roads, in cities, and at the workplace. Generated data can provide important insights to individuals—and to institutions—who use data to make predictions, improve services, and/or increase revenue through targeted advertisements (Wagner, 2018). Likewise, governments may collect data from multiple sources with the goal of ensuring national security; however, concerns about the intrusiveness of this data collection are widespread. For example, Edward Snowden’s revelations of mass government surveillance highlighted how the U.S. government monitors its citizens (Lyon, 2014), while the Chinese government has aggressively conducted state surveillance across the Internet (Xiao, 2019).

While such data collection and surveillance practices are common around the world, how individuals and governments think about privacy varies significantly. For example, the European Union (EU) passed the landmark General Data Protection Regulation (GDPR) in 2016, giving EU citizens more control over their data and creating new restrictions and reporting requirements for companies that collect personal data. These regulations differ significantly from the regulatory approaches in the United States, where most privacy laws are industry-specific, with no federal consumer privacy laws and only a handful of states instituting wide-ranging data privacy protections.

In this article, we explore differences in people’s attitudes toward privacy and data collection practices in the United States and the Netherlands, an EU member nation. Using a factorial vignette survey methodology and Nissenbaum’s (2009) theory of privacy as contextual integrity (CI) as a guiding framework, we identify specific contextual factors associated with people’s level of concern about how their data are being used. In our analyses, we address the following research questions:

RQ1: *How do trust and privacy attitudes toward data use vary across U.S. and Dutch respondents?*

RQ2: What differences and similarities emerge between U.S. and Dutch respondents in their data use concerns?

Applying the lens of CI, we interpret our findings and discuss how differences in social norms and legal landscapes shape attitudes toward data collection—and the wider implications of these differences. We conclude by noting that while U.S. and Dutch respondents differ in the personal data and data-related inferences they find concerning, they also share data privacy concerns—including their attitudes toward the dominance of U.S. platforms—that transcend national borders and contextual boundaries.

Related Work

We first highlight key privacy research in the United States and the EU, then describe CI and how we use it to frame our study.

Research on Privacy Attitudes, Knowledge, and Behaviors in the United States and the EU

Researchers have explored digital privacy attitudes, knowledge, and behaviors in U.S. and Dutch contexts. Americans' privacy attitudes are seemingly influenced by the presence of most of the world's largest technology companies as well as the country's policies regulating individual privacy rights. Researchers have highlighted that Americans have developed a sense of apathy, cynicism, and/or resignation toward privacy protections (e.g., Hargittai & Marwick, 2016; Hoffmann, Lutz, & Ranzini, 2016). The Pew Research Center found that a large proportion of Americans believe they have little to no control over who can access their location data, search history, online purchases, and even private messages (Auxier et al., 2019). Perhaps relatedly, Trepte and Masur (2016) found that almost half of the U.S. respondents in their cross-national comparative study experienced privacy violations on social media.

Dutch attitudes toward privacy and institutional trust are shaped by their recent sociopolitical context, including the absence of authoritarian regimes found in other EU member states (Zureik, Harling Stalker, Smith, Lyon, & Chan, 2010). Yet relative trust in the government does not preclude a sense of individual responsibility for privacy management among the Dutch: Research indicates that citizens feel the government and users themselves are the main actors responsible for data protection (Data Driven Marketing Association, 2018; Strycharz, Ausloos, & Helberger, 2020). Dutch citizens are most concerned about data typically associated with smartphones, such as search history, location data, messaging, and images, and less so with institutional data such as financial and medical records (Autoriteit Persoonsgegevens, 2019).

Concerning privacy knowledge, Dutch citizens report a comparatively strong recognition of European privacy protection regulations. About 80% of the Dutch population is aware of the Dutch Data Protection Authority and GDPR, putting them at the forefront of EU nations regarding their knowledge of privacy rights and the bodies that protect these rights (Kantar, 2019; Strycharz et al., 2020). While Strycharz and colleagues (2020) have noted that awareness does not guarantee understanding, Dutch awareness is high compared with Americans' knowledge of privacy regulations. A 2019 Pew survey found that nearly two-thirds of U.S. adults reported very little to no understanding of existing data protection laws (Auxier et al., 2019).

When it comes to privacy behavior, subjective privacy literacy was slightly higher among U.S. respondents compared with Dutch (Trepte & Masur, 2016). However, studies have highlighted that Americans have low digital literacy skills, especially in relation to the increasingly complex task of protecting personal data (e.g., Park, 2013; Smith, 2017). Dutch users balance a lack of confidence in their ability to protect their privacy with confidence in the range of protective behaviors available (Boerman, Kruikemeier, & Zuiderveen Borgesius, 2018). Moreover, Dutch participants found it slightly more important than U.S. respondents to prevent privacy violations (Trepte & Masur, 2016).

The current study builds on prior work comparing privacy perceptions, attitudes, and behaviors of U.S. and EU citizens (e.g., Trepte & Masur's 2016 cross-cultural comparative survey). It adds new insights by exploring the role of trust, privacy attitudes, and self-efficacy in shaping privacy attitudes and offers much-needed nuance by addressing the role contextual factors play.

CI as a Lens for Comparing Privacy Attitudes

Digital technologies introduce new flows of information that can challenge entrenched privacy norms and expectations. For example, the Cambridge Analytica scandal in 2018 spotlighted how data from one's social network activities might be used for psychometric profiling of political motivations (Cadwalladr & Graham-Harrison, 2018). A privacy concern emerged, in part because data disclosed in one context—communicating with friends and family—were unexpectedly used in a very different context—political ad targeting.

The challenges of negotiating privacy within and across contexts are central to Nissenbaum's (2009) theory of privacy as CI. CI posits that informational norms govern people's expectations of how data should flow within a given context. It identifies five parameters that shape norms: information attribute (type), subject (to whom the information pertains), sender (from whom the information comes), recipient (to whom information goes), and transmission principle (conditions that shape information flows). Contextual factors, such as what the data reveal (inference) and why the data are used (purpose) also shape informational norms. For example, people might be comfortable sharing their fitness data in a health context given norms regarding how such information is handled by healthcare professionals. However, if asked to share that same data with an employer, especially if that data were used to infer personal attributes, they might consider the data flow inappropriate.

Several researchers have operationalized CI's parameters in surveys to measure privacy expectations (Martin & Nissenbaum, 2020), identify privacy norms (Abdi, Zhan, Ramokapane, & Such, 2021; Shvartzshnaider et al., 2016), examine variations in privacy norms (Martin, 2012), evaluate whether privacy norms and regulations align (Apthorpe, Varghese, & Feamster, 2019), and compare privacy concerns across cultures (Utz et al., 2021). These studies demonstrate how perceived "inconsistencies" or "paradoxes" in privacy behaviors are the result of changes in the parameters of information flow rather than misunderstandings about the public availability or sensitivity of information. Several studies use factorial vignettes (explained in the next section) to pinpoint which parameter changes do and do not pose privacy concerns (Abdi et al., 2021; Martin, 2012; Martin & Nissenbaum, 2020; Utz et al., 2021). Combining CI and the factorial vignette method enables researchers to offer more nuanced explanations of when information flows raise questions.

In our study, we explore how attitudes toward subtle shifts in information norms might differ across cultures. The differences between legal and regulatory approaches to privacy between the United States and the EU have been well documented and analyzed (Bennett & Raab, 2006; Krotoszynski, 2016). Building on this, we consider whether the two cultural contexts also differ in how they respond to new information flows.

Method

The complexities inherent in privacy attitudes led us to pursue more innovative approaches to explore cultural variations. To do this, we used factorial vignettes, which bridge experiments and surveys (Wallander, 2009). In this method, respondents read short descriptions of scenarios and rate each scenario according to given criteria. Certain factors in each scenario are systematically varied, enabling researchers to study which factors affect people's judgments. This methodology is well-suited for studying nuanced social phenomena. Since changes in vignettes are subtle, respondents are less susceptible to social desirability bias seen in conventional surveys (Wallander, 2009). Compared with traditional survey research, factorial vignettes avoid non-orthogonal or collinear factors that occur in association with each other. Factorial vignette surveys are frequently used in research on complex judgments and beliefs in various contexts, especially pertaining to privacy (Abdi et al., 2021; Martin, 2012; Martin & Nissenbaum, 2020; Utz et al., 2021).

Constructing Vignettes

Drawing on prior factorial vignette studies that operationalize CI parameters (Martin, 2012; Martin & Nissenbaum, 2020), we identified five factors that shape people's privacy expectations: Actor (who is using the data), Content/Information Type (what kind of data is being used), Amount (how much data are being used), Inference (what the data reveal), and Purpose (why the data are used). Each factor contains different levels that provide variation in the scenarios. Table 1 lists the levels for each factor.

Table 1. Details of Vignette Factors.

Vignette Factors	# Levels	Factor Levels
Actor	6	Law enforcement
		Your company's human resources (HR) department
		Your doctor
		A social media/messaging app a respondent uses[2]
		An online advertising agency
		Your local government
Content/information type	8	Text-based posts and messages
		Photos and video posts
		Web browsing search history
		E-mails
		Phone's location data
		Social media posts
		Phone call log data
		Physical activity (inferred from phone stats)
Amount	3	One week's worth
		One year's worth
		The full history
Inference	6	Evaluate your mental state
		Evaluate how healthy you are
		Identify places you visit
		Infer who your friends are
		Infer your sexual orientation
		Infer your political views
Purpose of inferences	8	Preventing or reducing criminal activity
		Fighting terrorism
		Reducing the spread of disease
		Providing you with personalized advertising
		Improving traffic flow in your region
		Reducing people's engagement in binge drinking
		Creating a national database of citizens
		Increasing productivity

The initial vignette universe included 6,912 possible combinations: 6(Actor) × 8(Content) × 3(Amount) × 6(Inference) × 8(Purpose). Prior work recommends deleting vignettes that depict unrealistic

[2] Respondents were asked, "From the list of the below social media platforms, select the one you use the most," with eight response options (plus "Other"). Their response was inserted in any vignettes that included social media/messaging app as the actor.

scenarios (Wallander, 2009); studies that include "unrealistic" descriptions may generate unrealistic results since the respondents, when presented with unusual combinations of dimension levels, may start making judgments that do not accurately reflect the principles that they would have used had the vignettes been realistic (Faia, 1980). We removed unrealistic scenarios (e.g., "Your doctor" × "Improving traffic flow in your region") from the corpus, leaving 5,232 combinations. Vignette texts were generated automatically and uploaded to the survey platform Qualtrics.

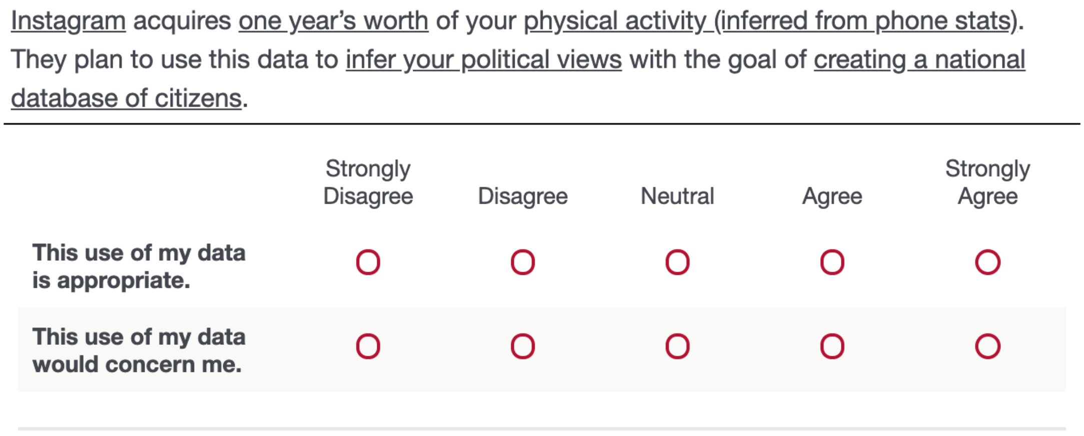
Data Collection

Survey data were collected in May 2019. American respondents were recruited from Amazon Mechanical Turk, while Dutch respondents were recruited through IPSOS. Numerous U.S.-based studies have used Mechanical Turk, with Martin and Nissenbaum (2020) finding that it produced "the same theoretical generalizations" (p. 287) as a national survey of privacy attitudes. The Dutch sample is representative of the Dutch population.

Each respondent first answered questions about their background and views on privacy, trust, and data collection, then viewed and rated 32 randomly selected vignettes across two dimensions (see Figure 1 for a sample vignette as it appeared to the respondents). After the removal of incomplete and low-quality responses, the final data set included 10,433 vignette responses from 329 U.S. respondents and 14,588 responses from 511 Dutch respondents.

Ethical Considerations

Protocols for data collection were approved by appropriate ethical review boards at both the U.S. and Dutch institutions, and standard steps were taken to ensure respondent anonymity and confidentiality. Following Pittman and Sheehan (2017), our use of Mechanical Turk and IPSOS followed existing best practices for fair and ethical compensation of participants.



Instagram acquires one year's worth of your physical activity (inferred from phone stats). They plan to use this data to infer your political views with the goal of creating a national database of citizens.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
This use of my data is appropriate.	○	○	○	○	○
This use of my data would concern me.	○	○	○	○	○

Figure 1. Example vignette as it appeared to respondents.
Note. Underlined text indicates the factors that varied between vignettes.

Measures: Dependent Variables

For each vignette, respondents' attitudes were measured across two dimensions of privacy along a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree): *Data Use Concern* (United States: $M = 4.20$, $SD = 1.07$; Dutch: $M = 3.95$, $SD = 1.20$) and *Perceived Appropriateness of Data Use* (United States: $M = 1.70$, $SD = 1.00$; Dutch: $M = 1.72$, $SD = 1.01$). For Data Use Concern, a higher value indicates greater data privacy concerns associated with the presented scenario. For Appropriateness of Data Use, a higher value indicates the data use was perceived as more appropriate. As expected, these two variables were negatively correlated, $r = -.58$, $p < .001$; in other words, the more concerned a respondent was regarding a particular use of data, the less appropriate they rated that scenario.

In this article, we only report findings from analyses using Data Use Concern as the dependent variable (DV). The first reason is to avoid redundancy. Based on initial mixed-effects modeling using the U.S. sample, we found significant factors echoed in both models with the opposite effect on levels of data use concern and perceived appropriateness. Additionally, because the word "appropriate" does not have a direct translation in Dutch, we used the alternative Dutch word "*gerechtvaardigd*," which emphasizes legality rather than norms. We chose to focus on Data Use Concern to make the cross-cultural comparative analyses more robust and reliable.

Measures: Independent Variables

We captured the following variables in our survey to control for the influence of trust, privacy attitudes, and self-efficacy in shaping people's attitudes toward various data collection scenarios.

Trust in Social Institutions

To measure trust in social institutions, we used a 5-point Likert scale to measure respondents' trust toward local and federal governments, U.S. companies, social media platforms, and the news media (United States: $M = 2.52$, $SD = .96$, $\alpha = .88$; Dutch: $M = 2.80$, $SD = .89$, $\alpha = .89$). Response options ranged from 1 (Strongly Disagree) to 5 (Strongly Agree). See Table 2 for items.

Mobile Privacy Concerns

To measure privacy concerns, we employed Xu, Gupta, Rosson, and Carroll's (2012) validated scale (United States: $M = 3.95$, $SD = .65$, $\alpha = .91$; Dutch: $M = 3.89$, $SD = .70$, $\alpha = .92$). Respondents were asked to rate their level of agreement with eight statements[3] (Table 3). Response options ranged from 1 (Strongly Disagree) to 5 (Strongly Agree), with a higher value indicating a higher level of mobile privacy concern.

[3] The scale developed by Xu and colleagues (2012) includes nine statements; we used one ("I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy") as an attention-check item. Therefore, our scale only includes eight items.

Self-Efficacy Related to Online Privacy

Self-efficacy (United States: *M* = 64.74, *SD* = 22.40, *α*=.88; Dutch: *M* = *52*.11, *SD* = 19.74, *α*=.90) was measured via an original three-item scale. The survey asked respondents to rate their level of confidence in (1) knowledge of how to safeguard their privacy and security online (e.g., clearing Web browser history); (2) knowledge of various types of data their phone shares with mobile apps; and (3) ability to control what and how information is shared online. Responses were recorded on a slider scale from 1 (Not at all confident) to 100 (Completely confident).

Privacy Fatalism and Pragmatism

Privacy fatalism (United States: *M* = 2.41, *SD* = .75, *α* =.74, Dutch: *M* = *2*.88, *SD* = .68, *α*=.80) was measured using a four-item scale capturing the extent to which respondents believed privacy no longer exists. Privacy pragmatism (United States: *M* = 2.47, *SD* = 1.06, *α* =.79, Dutch: *M* = *2.63*, *SD* = 1.04, *α*=.84) was measured using a two-item scale capturing the extent to which respondents would exchange privacy for some benefit (Table 4). Responses for all items were recorded on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

Control Variables

We included three control variables: Gender identity, age, and education. Respondents in the U.S. sample were more likely to be male (60%), with an average age of 36.45 years (*SD* = 10.52, range: 18–72). Most respondents had a bachelor's (54.6%) or graduate (12.7%) degree. Among the Dutch sample, 49% were male and the average age was 46.13 (*SD* = 14.16, range: 18–66). In line with general education levels in the Netherlands (Maslowski, 2020), 41% of the respondents were highly educated (29% had a bachelor's degree, 12% an advanced degree) whereas 38% reported a vocational/associate degree, and 22% did not have education beyond the high school level.

Data Analysis

We used a combination of R (lme4 package) and SPSS to perform data analysis. Our factorial survey sampled both respondents and vignettes. Therefore, data were generated at two distinct levels: individual and vignette. To accommodate the hierarchical structure of this data set, we used mixed-effects modeling to account for within- and between-subject differences (Hox, Kreft, & Hermkens, 1991). It is important to note that all vignette- and respondent-level variables can possibly modify the judgment threshold, so we included both individual characteristics (e.g., age, trust, privacy beliefs) and vignette factors in the final models to explain variances of data use concern.

Since each factor contains multiple levels, we conducted Bonferroni pairwise comparisons to examine differences in the level of concern based on the type of actors, content, amount, inference, and purpose of data use. However, U.S. respondents reported greater concerns across all vignette factors. With such differences in the threshold of judgment, we need to go beyond simply comparing the absolute value of means. Therefore, we calculated z-scores to provide a way of standardizing data across a wide range of experimental conditions (DeVore, 2017) and allow for more meaningful cross-cultural comparative analyses. A z-score of zero represents the population means of concern based on each factor (adjusted by controlling for other factors and covariates). Negative z-scores indicate that respondents felt more concerned, and positive z-scores indicate that respondents felt less concern regarding a given factor.

Results

RQ1: Evaluating Cultural Differences in Trust and Privacy Beliefs

Compared with the Dutch sample, Americans reported significantly lower trust in social institutions. When looking at individual items, Americans reported significantly lower trust in the federal government, local government, social media platforms, and the news media. Both American and Dutch respondents reported low trust in U.S. companies. Results from *t*-tests are shown in Table 2.

Table 2. Comparing Respondents' Trust in Social Institutions.

Variable	Item Wording		**American** (n = 324)	**Dutch** (n = 507)	***t***	***p***
Trust in federal government	Most of the time I trust people in my federal government to do what is right.	*M*	2.63	3.15	−6.33	<.001
		SD	1.16	1.14		
Trust in local government	Most of the time I trust people in my local government (including law enforcement) to do what is right.	*M*	2.86	3.15	−3.67	<.001
		SD	1.20	1.09		
Trust in U.S. companies	Most of the time I trust American companies to do what is best for consumers.	*M*	2.27	2.29	−.23	.82
		SD	1.14	1.14		
Trust in the social media platform	Most of the time I trust [social media platform] to do what is best for consumers.	*M*	2.15	2.53	−4.75	<.001
		SD	1.14	1.11		
Trust in the news media	Most of the time I trust the news media to do what is right in their reporting.	*M*	2.7	3.05	−4.14	<.001
		SD	1.21	1.11		
Full scale	Average score across five trust items	*M*	2.52	2.83	−4.77	<.001
		SD	0.89	0.96		

Note. On a 5-point Likert scale, 1 = strongly disagree, 5 = strongly agree.

Both samples reported a relatively high degree of mobile privacy concerns, with each item scoring around four out of five points. Compared with the Dutch, Americans reported significantly higher privacy concerns for five of the eight items on Xu and colleagues' (2012) scale as well as for the full scale. Item means and *t*-test results are in Table 3.

Table 3. Comparing Respondents' Mobile Privacy Concerns.

			American	**Dutch**		
Variable	Item Wording		(n = 324)	(n = 507)	***t***	***p***
Mobile concern 1	I believe that the location of my mobile device is monitored at least part of the time.	*M*	4.09	3.89	3.2	<.001
		SD	0.77	0.97		
Mobile concern 2	I am concerned that mobile apps are collecting too much information about me.	*M*	4.09	3.94	2.23	.03
		SD	1.00	0.92		
Mobile concern 3	I am concerned that mobile apps may monitor my activities on my mobile device.	*M*	3.96	3.94	0.32	.75
		SD	.99	1.02		
Mobile concern 4	I feel that as a result of my using mobile apps, others know about me more than I am comfortable with.	*M*	3.84	3.6	3.42	<.001
		SD	1.00	0.92		
Mobile concern 5	I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.	*M*	3.98	3.74	3.62	<.001
		SD	0.94	0.93		
Mobile concern 6	I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.	*M*	4.18	4.07	1.85	.06
		SD	0.88	0.87		
Mobile concern 7	When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.	*M*	4.15	3.85	4.77	<.001
		SD	0.91	0.89		
Mobile concern 8	I am concerned that mobile apps may share my personal information with other entities without getting my authorization.	*M*	4.16	4.08	1.23	.22
		SD	0.92	0.89		
Full scale	Average of eight mobile concern items	***M***	**4.06**	**3.89**	**3.35**	**<.001**
		SD	**0.73**	**0.70**		

Note. On a 5-point Likert scale, 1 = strongly disagree, 5 = strongly agree.

Dutch respondents reported a statistically higher level of resignation/fatalism related to online privacy; comparing the four-item privacy fatalism scale, Dutch reported greater agreement (*M* = 2.88, *SD* = .68) than Americans (*M* = 2.41, *SD* = .75) with statements that reflected a belief that privacy no longer exists or there is little to be done to prevent privacy invasions, *t*(829) = −9.28, *p* < .001. Likewise, Dutch respondents (*M* = 2.63, *SD* = 1.04) reported a higher degree of pragmatism related to online privacy compared with U.S. respondents (*M* = 2.47, *SD* = 1.06), *t*(829)=2.10, *p* < .05. In other words, the Dutch were more willing to trade their data for convenience or a reduced cost of service than Americans. Item means and *t*-test results are shown in Table 4.

Table 4. Comparing Respondents' General Privacy Attitudes.

			American	**Dutch**		
Variable	Item wording		(n = 324)	(n = 507)	***t***	***p***
Fatalism belief 1	There is nothing I can do to protect my privacy and security online.	*M*	2.20	2.64	−6.12	<.001
		SD	0.99	1.02		
Fatalism belief 2	In the online world, privacy does not exist anymore.	*M*	2.86	3.15	−8.33	<.001
		SD	0.89	1.02		
Fatalism belief 3	There's nothing I can do to prevent my account from being hacked.	*M*	2.27	2.29	−5.91	<.001
		SD	0.97	1.05		
Fatalism belief 4	I have control over the information I share online. [reverse coded]	*M*	2.15	2.53	−5.6	<.001
		SD	0.89	0.97		
Full scale	Average score of four privacy fatalism scale items	*M*	2.41	2.88	−9.28	<.001
		SD	0.75	0.68		
Pragmatism belief 1	I might trade my personal data for convenience.	*M*	2.50	2.61	1.27	.20
		SD	1.13	1.10		
Pragmatism belief 2	I might give my personal data for a reduced cost of service.	*M*	2.44	2.65	2.41	.02
		SD	1.20	1.17		
Full scale	Average score of two privacy pragmatism scale items	*M*	2.47	2.63	2.10	.04
		SD	1.06	1.04		

Note. On a 5-point Likert scale, 1 = strongly disagree, 5 = strongly agree.

RQ2: Explaining Data Use Concerns: Differences and Similarities

For our second research question, we examined differences in factors that influenced U.S. and Dutch respondents' concerns about their data use, using the data generated from responses to more than 25,000 vignettes across our two samples. As shown in Table 5, the final models contain both fixed (between-subject) and random (within-subject) effects. These statistically significant parameters suggest that respondents' data use concerns were influenced by both vignette attributes and individual characteristics. These fixed effects for the final mixed models were interpreted in the same way as regression analysis of variance or analysis of covariance, depending on the nature of these explanatory variables (Seltman, 2012).

Table 5. Linear Mixed-Effects Models (DV = Data Use Concern).

	American		**Dutch**	
Fixed Effect (Between-subject)	***F***	**Sig.**	***F***	**Sig.**
Intercept	42.92	<.001	56.16	<.001
Individual Characteristics				
Age	6.53	<.01	13.78	<.001
Gender (= male)	0.01	.97	0.64	.42
Education	1.00	.32	3.62	.06
Mobile privacy concern	81.86	<.001	30.71	<.01
Trust	4.33	<.05	0.01	.93
Self-efficacy	0.37	.54	0.00	.99
Fatalism belief	4.12	<.05	13.03	<.001
Pragmatism belief	5.83	<.05	3.5	.06
Vignette Attributes				
Actor	7.68	<.001	45.81	<.001
Amount	21.98	<.001	0.60	.55
Content	15.00	<.001	1.83	.08
Inference	19.29	<.001	13.15	<.001
Purpose	19.12	<.001	17.98	<.001
Random effect (Within-subject)[a]	**Wald Z**	**Sig.**	**Wald Z**	**Sig.**
Residual	70.66	<.001	78.77	<.001
Intercept	12.21	<.001	14.72	<.001
Model fit Bayesian information criterion (BIC)[b]	BIC =23610.31		BIC=28808.12	

[a] Wald *Z* tests determine if the random intercept is needed. In our case, null hypotheses of no random effect are rejected, with p < .001. We do need to include a random intercept.

[b] BIC is an estimator of prediction error. Lower values indicate better model performance. We compared and selected the most optimal models.

Cross-Country Comparison: Role of Individual Characteristics

Table 6 presents more detailed model results to unpack how individual characteristics might shape consumer concerns about data use.

Table 6. Estimated Effects of Individual Characteristics on Data Use Concern.

	American	**Dutch**
	Standardized Coefficients	
Age	.01*	.01*
Gender (= male)	0	−.07
Education	.02	.11
Mobile privacy concern	.49***	.37***
Trust	−.09*	0
Self-efficacy	0	0
Fatalism belief	−.11*	−.25***
Pragmatism belief	−.09*	.08

** p <.05, ** p <.01, *** p <.001.*

The patterns of individual characteristics that influence data use concerns are similar among U.S. and Dutch respondents. In both groups, older respondents and those who expressed greater mobile privacy concerns were more likely to find a given data use scenario concerning, while people who reported higher levels of privacy fatalism were less concerned about data use. Education, gender, and self-efficacy were not significant predictors in either sample.

The differences regarding the effects of individual characteristics manifest in the level of trust and privacy pragmatism, both of which were statistically significant in the U.S. sample but not in the Dutch. Additionally, mobile privacy concerns had a larger effect among U.S. respondents, while a sense of fatalism had a larger effect among Dutch respondents.

Cross-Country Comparison: Roles of Data Use Context

Respondents' concerns about data use varied by vignette attributes. Table 7 lists the effects (estimated coefficient) of each dimension of vignette factors on the level of data use concern. Note that these effects should be interpreted using a reference level within each type of vignette factor; for example, compared with their local government, Americans viewed data use by social media platforms as less concerning and their company's HR department as more concerning.

Table 7. Model Details: Estimated Effects of Vignette Factors on Data Use Concern.

	American	**Dutch**
	Standardized Coefficients	
Actors		
An online data broker	−.01	.10**
Social media (most frequently used platform)	−.09**	−.05
Law enforcement	−.02	−.11***
Your company's HR department	.06*	.15**
Your doctor	−.05	−.02

Your local government	—[a]	—[a]
Content		
E-mails	.08**	.03
Phone call log data	.01	.03
Phone’s location data	−.05	.02
Photos and video posts	−.01	.08
Physical activity (inferred from phone stats)	−.16***	.02
Social media posts	−.12***	−.03
Text-based posts and messages	0	.04
Web browsing search history	—[a]	—[a]
Amount		
One week’s worth	−.11***	−.01
One year’s worth	−.02	0
The full history	—[a]	—[a]
Inference		
Evaluate how healthy you are	−.23***	−.11***
Evaluate your mental state	−.1***	−.11***
Identify places you visit	−.2***	−.17***
Infer who your friends are	−.11***	−.07**
Infer your political views	−.09**	−.07**
Infer your sexual orientation	—[a]	—[a]
Purpose		
Creating a national database of citizens	.19***	.05*
Fighting terrorism	.05	−.14***
Improving traffic flow in your region	−.29**	−.18***
Increasing productivity	.03	.03
Preventing or reducing criminal activity	.09***	−.06**
Providing you with personalized advertising	.09**	.05
Reduce binge drinking	.02	.05*
Reducing the spread of disease	—[a]	—[a]

[a] Reference category for that factor.
$*p < .05$, $**p < .01$, $***p < .001$.

To directly differentiate levels of concern across the U.S. and Dutch samples, we conducted a series of Bonferroni pairwise comparisons across each level of factors. Estimated means of data use concern were calculated for each type of factor while adjusting for other covariates (e.g., age and mobile privacy concerns) and the random effects (i.e., repeated assessments by each respondent). Values were then transformed to z-scores to allow for more meaningful comparisons.

Effects of Actor Type

First, we looked at the actor involved in data collection, using six groups that might collect personal data. The overall models highlight significant effects of actor type on data use concerns: U.S. respondents: $F(5,9992) = 7.68$, $p < .001$; Dutch respondents: $F(5,12415) = 45.84$, $p < .001$. Figure 2 shows z-scores for normalized data use concern values across the six types of actors.

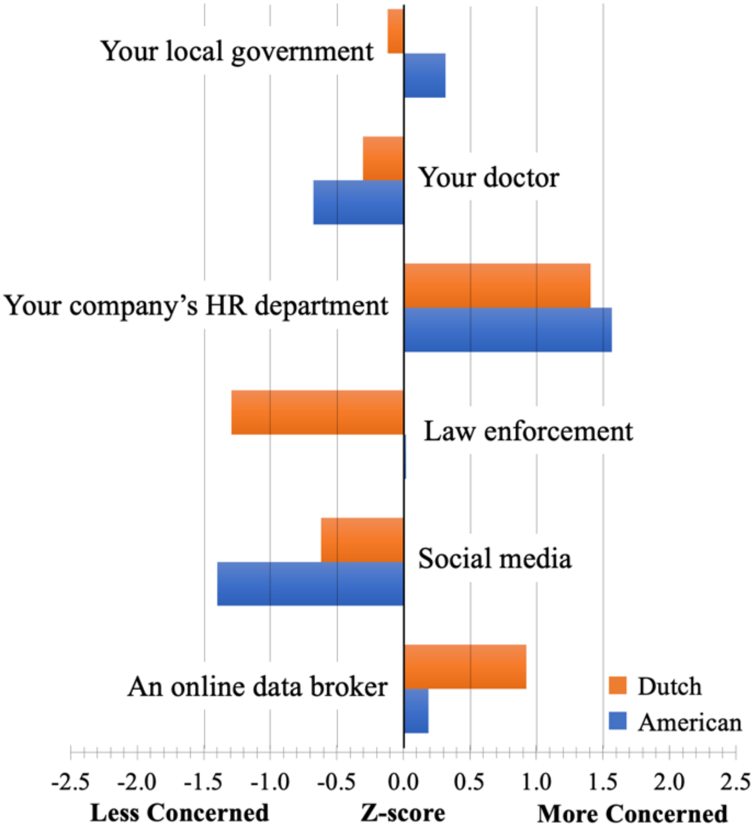


Figure 2. Normalized z-scores of data use concerns by actor.

Dutch respondents reported lower concern when actors were local government or law enforcement, while Americans felt more concerned about data use by these two actors. Both U.S. and Dutch respondents expressed greater concern about data use by their company's HR department and an online data broker. Dutch respondents felt more concerned about data use by online data brokers compared with Americans. Both U.S. and Dutch respondents felt less concerned about data use by their doctor and social media, but the degree of concern was lower among Americans.

Effects of Content Types

The effect of content type on the level of concern was statistically significant among U.S. respondents: *F*(7,10008) = 15.00, *p* < .001. However, for the Dutch sample, content type was not significant: *F*(7,12425) = 1.83, *p* = .08. Using the normalized values, we compared the two samples and identified several similarities and differences. Figure 3 shows standardized z-scores of data concern based on types of content.

Dutch respondents were less concerned about the use of search history data compared with Americans. Both Dutch and U.S. respondents reported higher concerns about data use related to their text-based posts and messages, photo and video posts, phone call log data, and e-mails. However, the Dutch were significantly more concerned about their photo and video posts, while Americans were more concerned about e-mails. Conversely, both samples were less concerned about social media posts, physical activity data, and phone call log data, but U.S. respondents appeared to care less about physical activity data and more about their social media posts compared with Dutch respondents.

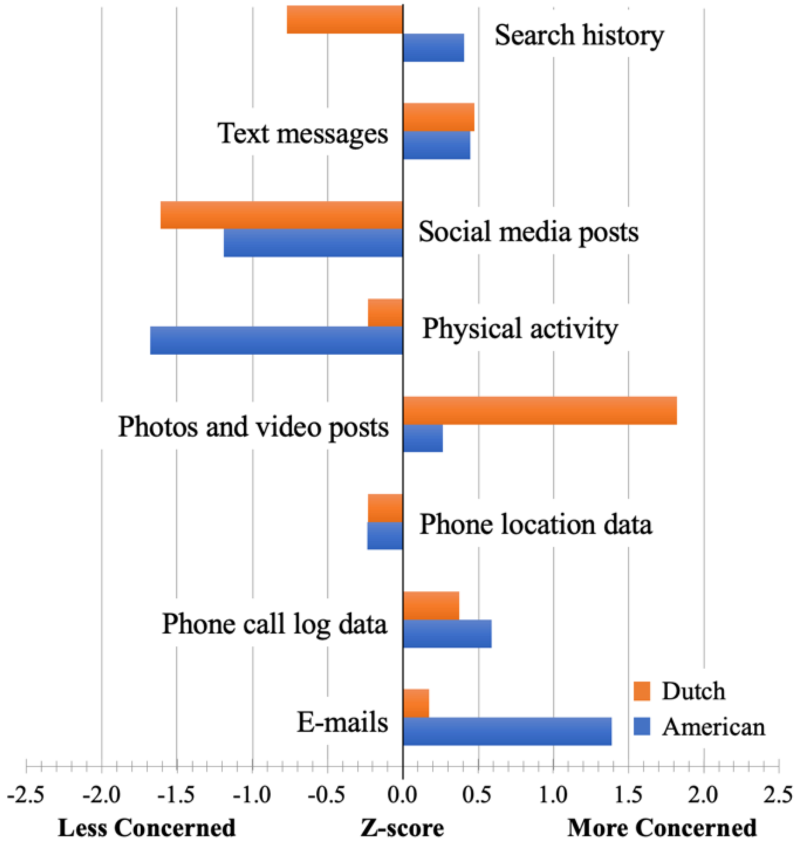


Figure 3. Normalized z-scores of data use concerns by content.

Effects of Data Quantity

The effect of the amount of data being collected was statistically significant for U.S. respondents, *F*(2, 10007) = 21.99, *p* < .001, but not for Dutch, *F*(2, 12424) = .60, *p* = .55. Figure 4 shows standardized z-scores based on the amount of data used. Both U.S. and Dutch respondents expressed less concern about one week's worth of data being used, but more concern about one year's worth or their full data history.

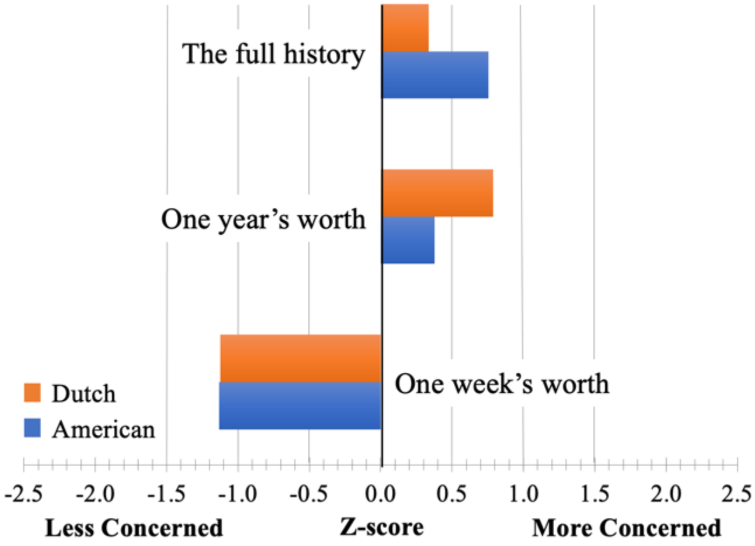


Figure 4. Normalized z-scores of data use concerns by data amount.

Effects of Inference Types

The effects of the inference being made on data use concerns were statistically significant for both samples [U.S. respondents: *F*(5, 10009) = 19.29, *p* < .001; Dutch respondents: *F*(5, 12415) = 13.15, *p* < .001]. Figure 5 shows standardized z-scores based on type of inference. The only cross-cultural difference observed was inferring mental state: Americans felt more concerned when data were used to infer their mental state, while the Dutch felt less concerned. Otherwise, both Americans and Dutch felt more concerned when data were used to infer their sexual orientation, political views, and friend network. Conversely, both samples felt less concerned when data were used to infer places that they visited and their overall health although Americans were significantly less concerned than Dutch about health-based inferences.

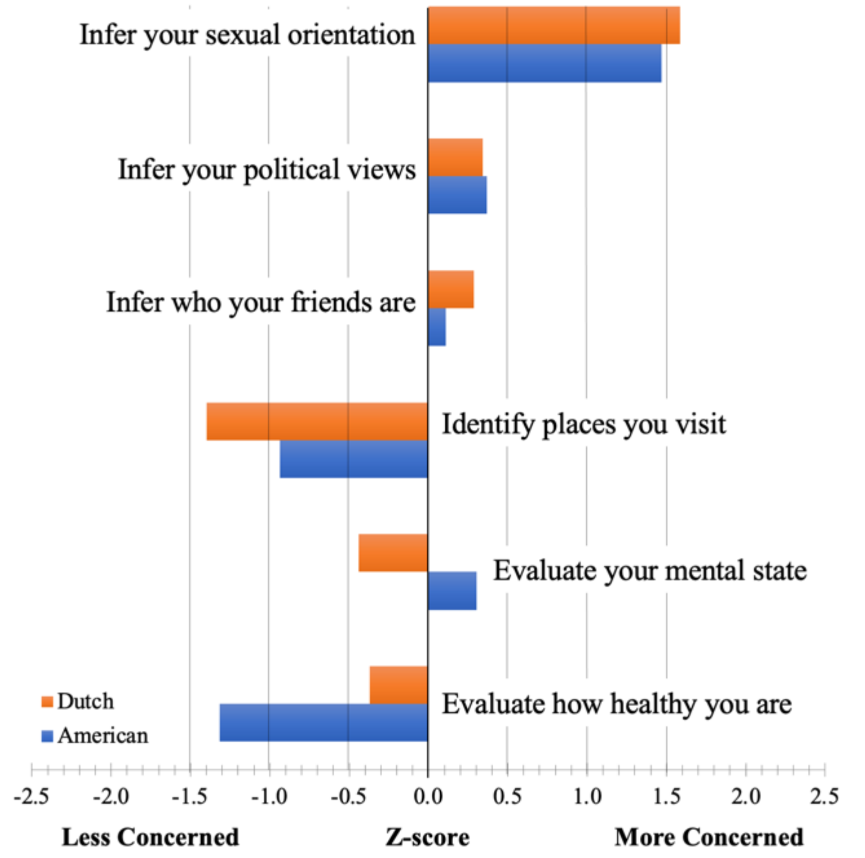


Figure 5. Normalized z-scores of data use concerns by inference.

Effects of Purpose Types

The effect of purpose on data use concerns was significant for both samples, U.S. respondents: *F*(7, 10009) = 19.12, *p* < .001 and Dutch respondents: *F*(7, 12425) = 17.98, *p* < .001, with several differences in how American and Dutch respondents reacted to various data use purposes. Figure 6 shows standardized z-scores based on purpose.

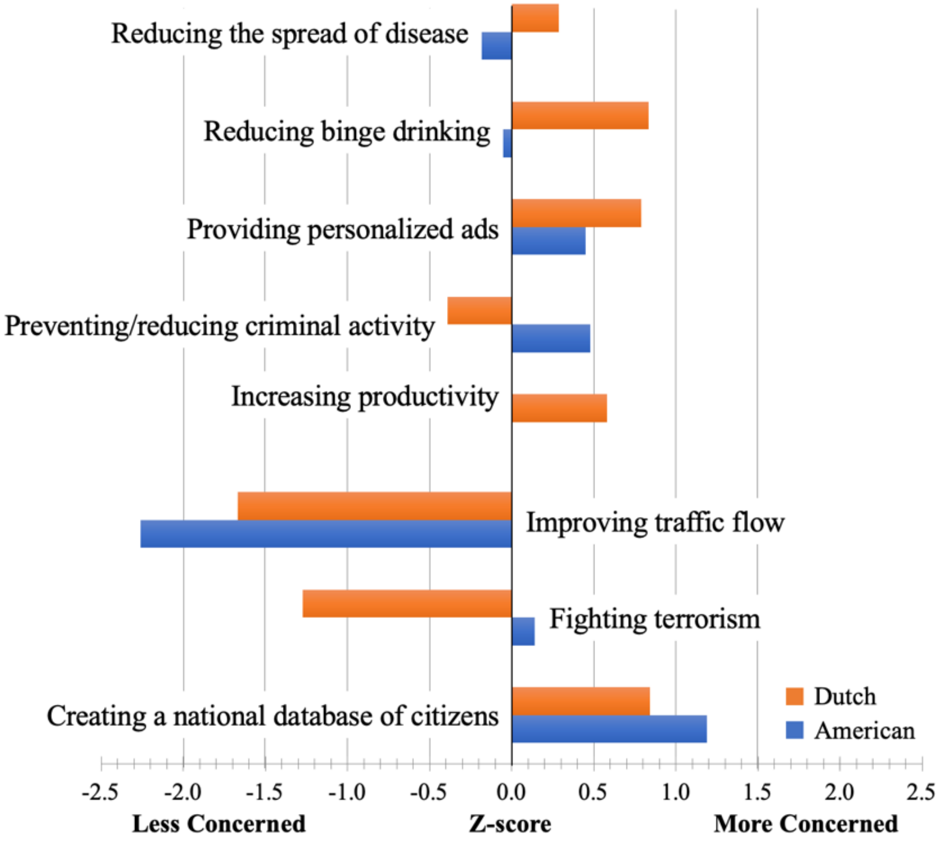


Figure 6. Normalized z-scores of data use concerns by purpose.

Dutch respondents were less concerned about data use for two purposes related to public safety: Preventing or reducing criminal activity and fighting terrorism. However, Americans considered these two purposes more concerning. The Dutch were more concerned about reducing the spread of disease and reducing binge drinking, while Americans were less concerned about these two purposes. In terms of cross-cultural similarities, both U.S. and Dutch respondents expressed greater concerns when data were collected for providing personalized advertising and creating a national database for citizens. And both became less concerned about using data to improve local traffic.

Discussion

Through factorial vignette surveys in the United States and the Netherlands, we explored cross-cultural variations in people's trust, privacy attitudes, and data use concerns across a variety of contextual factors. Such evaluations are increasingly important as countries respond to advances in ICTs with varied approaches to defining basic privacy rights and protecting citizens' data. In this study, we used CI

(Nissenbaum, 2009) as a guiding framework to evaluate cross-cultural variations and identify factors that are more or less likely to raise concerns in the two countries.

Our analyses revealed cross-cultural differences in trust toward the government, with Dutch respondents placing greater trust in their government than Americans. This finding might be due to the stronger presence of the Dutch government in the public sphere, as demonstrated by government-initiated welfare policies in the Netherlands (Hicks, 2018). Likewise, Americans' lower trust in government aligns with a broader trend of declining trust and disapproval of government intervention (Rainie, Keeter, & Perrin, 2019). On the other hand, both U.S. and Dutch respondents expressed low trust that U.S. companies do what is best for consumers. This finding is unsurprising given recent data scandals (e.g., Cadwalladr & Graham-Harrison, 2018).

We also identified several differences when looking at privacy attitudes. Compared with Americans, Dutch respondents expressed lower privacy concerns, which might be explained by their higher level of fatalism and pragmatism, alongside the belief that EU regulations would protect citizens from more egregious privacy violations. In fact, Americans consistently reported greater privacy concerns on every item in Xu and colleagues' (2012) mobile privacy concern scale. This raises important questions as to whether the presence—or relative absence, in the U.S. case—of strong regulatory frameworks alone explains these differences, or if other factors may inflate Americans' concerns about their data. Future research should consider how factors like media coverage of privacy events (e.g., data breaches), digital literacy, and general knowledge of privacy regulations shape Americans' attitudes toward privacy. The GDPR is reasonably well-known throughout the EU (Kantar, 2019), while nearly two-thirds of U.S. adults report knowing little to nothing about U.S. privacy laws (Auxier et al., 2019).

Turning to our vignettes, Nissenbaum (2009) identifies a number of parameters that influence the perceived appropriateness of an information flow within a given context. Variance in any of these parameters might constitute a disruption in the "contextual integrity" of the norms of information flow, triggering a privacy concern. This contextual approach to privacy permits a more robust understanding of the complex ways individuals consider appropriateness of personal data flows across various scenarios, and numerous scholars have used CI to understand variations in privacy attitudes and practices in a range of contexts. We extend this prior work by further examining variations between two countries with different social norms and legal landscapes for regulating data collection and use.

First, we consider the actors involved in data exchange; in our study, this was the recipient of data or the organization collecting it. While U.S. and Dutch respondents expressed similarly high concerns about data collected by their employer's HR department and generally expressed fewer concerns about doctors, they varied on all other actors. Most notably, the Americans were more concerned than the Dutch about law enforcement and local government actors. This pattern ties back to the general distrust Americans have for various government agencies (Rainie et al., 2019), which is not as prevalent in the Netherlands.[4] Across all

[4] These results may have shifted since data collection. Dutch citizens' trust in local governments decreased significantly due to their handling of the pandemic, alongside racial profiling scandals by tax authorities (Engbersen et al., 2021).

respondents, there was generally low concern about data collected by social media, likely because people are aware of data being collected on these platforms, and they may not view that data as sensitive—or they may feel resigned to data collection, knowing they have little control over what gets shared (Auxier et al., 2019; Hargittai & Marwick, 2016; Hoffmann et al., 2016).

Second, the CI framework indicates that type and amount of information being shared influence whether an information flow is viewed as appropriate. Regarding data quantity, respondents' concern increased as the length of time increased. This makes sense as more data are generated over time, and a greater quantity of data could signal greater risks. For example, Fiesler and Proferes (2018) found that Twitter users' discomfort increased as more data were collected about them; we would expect similar discomfort for data collected from other data types.

Building on our social media actor findings, both U.S. and Dutch respondents reported low concerns about their social media posts and physical activity data being collected. This finding aligns with prior work that people who use fitness wearables view generated data (e.g., steps, pulse) as innocuous (Zimmer, Kumar, Vitak, Liao, & Chamberlain Kritikos, 2020). On the other hand, prior work looking more narrowly at different types of social media content identified variations in users' concerns about different types of data. For example, sensitive or personal Facebook posts were more concerning than more generic posts about food (Gilbert, Vitak, & Shilton, 2021). Considered alongside this prior work, our findings highlight the increasing complexity faced by individuals seeking to manage their privacy and personal information flows.

Third, CI considers whether data flows align with existing norms of appropriateness within a particular context. We evaluated contextual appropriateness through the inferences drawn from data collected and the purpose of that analysis. U.S. and Dutch respondents were largely in agreement regarding inferences, with one notable exception: Using data to evaluate mental state was seen as less concerning by Dutch and more concerning by Americans. Technology is already used to infer mental illnesses (Huckins, 2020) and, in some cases, act on algorithmically determined mental health crises (Goggin, 2019). The lack of regulation of algorithms and artificial intelligence in the United States may lead Americans to have greater concerns about the potential uses of these technologies, while greater access to healthcare and social services in the Netherlands might reduce their concerns about evaluations of one's mental state.

Looking at the purpose of these inferences, we observed general agreement that improving traffic was not concerning, while providing personalized advertising and creating a database of citizens were more concerning. Other purposes, however, revealed differences between our respondents. The Dutch showed more concern—and Americans less concern—when data were used to reduce the spread of disease and reduce binge drinking. This discrepancy seems to imply a Dutch skepticism of public health initiatives although the type of institution handling personal data for such purposes may provide context. While Dutch respondents in one study cited doctors as the most trustworthy with personal information (Data Driven Marketing Association, 2021), a separate study reports that insurance companies are among the most troubling organizations when it comes to the misuse of personal data (Autoriteit Persoonsgegevens, 2019). Likewise, there was significant concern in the Netherlands in the early months of the COVID-19 pandemic regarding the development of a contact tracing app, with some experts arguing it would not meet privacy requirements (Loohuos, 2020).

On the other hand, Americans grew more concerned—and the Dutch less concerned—when data were used for two public safety purposes: fighting terrorism and preventing criminal activity. Heightened concern among Americans might be associated with growing disapproval of government surveillance in the aftermath of Edward Snowden's disclosures regarding global surveillance programs (Madden & Rainie, 2015). Conversely, Dutch public discourse finds critical framings coexisting with more accepting attitudes toward surveillance in the post-Snowden context (Mols & Janssen, 2017). This might also connect with the Dutch orientation toward pragmatism, which would anticipate that governments adhere to regulatory boundaries. As such, within legal limits, the use of data for safety and security may be expected and accepted.

Overall, these findings point to notable cultural differences in how these two populations make trust and risk determinations with respect to the use of their personal data. Dutch respondents place a higher degree of trust in their own government, and both American and Dutch respondents distrust U.S. companies. We also observed divergence in attitudes toward purposes of data use, with the Dutch having more concern with public health initiatives and Americans expressing more concern about their data being used to combat crime and terrorism. Through our application of CI, these findings reveal how respondents in these two countries articulate different contextual norms and data privacy concerns, which suggests the need for more nuanced approaches that account for cultural variations when predominantly platforms developed by the United States spread globally.

Study Strengths and Limitations

As a bridge between experiments and surveys, factorial vignettes carry the strengths and weaknesses of both types of empirical work. The highly controlled nature of the vignettes ensures greater internal validity than in usual surveys, and they capture the complexities of privacy-related norms and decision-making while being less susceptible to social desirability bias (Martin, 2012; Wallander, 2009). However, pervasive cultural or personality differences may also explain the variances between contracting groups' responses (Martin, 2012). We attempted to mitigate these incongruences by using mixed-effects modeling to account for individual differences within each group. In addition, the differences in sample representativeness may have implications for the degree of comparability between U.S. and Dutch data. Finally, the results point to respondent attitudes rather than their expected behaviors. Future qualitative research could begin unpacking the findings from our study.

Conclusion

While ICTs are increasingly accessible worldwide, how countries regulate companies and protect citizens' data varies significantly. In this article, we compared people's privacy concerns regarding data use in two different regulatory contexts—the United States and the EU—using factorial vignettes to identify how various contextual factors influence respondents' privacy concerns. We argue that such cross-cultural analyses are important for understanding how privacy attitudes and behaviors are enacted throughout the world and for raising important questions for companies and policymakers to address in the design and regulation of new technologies.

By using CI as a guiding framework in our study design, we isolated how U.S. and Dutch respondents consider the appropriateness of data collection and use across multiple variables and contexts. This approach provided a more nuanced understanding of how such contextual attitudes compare across these cultures. That said, Nissenbaum's (2009) theory, by itself, does not explain *why* such differences exist. We hope future research explores the underlying causes of these differences and provides recommendations for mitigating data privacy concerns. One factor that likely plays a role is the European approach to privacy regulation. With a focus on protecting consumer data and empowering citizens to have greater control over who can access their data, the EU's consumer-focused protections likely reduce some privacy concerns. While the United States does not yet have comprehensive privacy legislation, the California Consumer Privacy Act took effect in 2020. This state law will provide important insights into what federal regulations in the United States might look like, and future work should continue to monitor how developments in U.S. privacy legislation correlate with changes in attitudes and behaviors.

References

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021). Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Article No. 558). New York, NY: ACM. doi:10.1145/3411764.3445122

Apthorpe, N., Varghese, S., & Feamster, N. (2019). Evaluating the contextual integrity of privacy regulation: Parents IoT toy privacy norms versus COPPA. In *Proceedings of the 28th USENIX Security Symposium* (pp. 123–140). Berkeley, CA: USENIX Association.

Autoriteit Persoonsgegevens. (2019). *Nederland maakt zich zorgen over privacy. Flitspeiling privacyrechten* [The Netherlands is concerned about privacy. Flash poll privacy rights]. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/resultaten_enquete_privacyzorgen_jan_2019.pdf

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. Cambridge, MA: MIT Press.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research, 48*(7), 953–977. doi:10.1177/0093650218800915

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Data Driven Marketing Association. (2018). *DDMA privacy monitor: Wat consumenten denken* [DDMA privacy monitor. What consumers think]. Retrieved from https://www.retailinsiders.nl/docs/b7de5213-7934-47b7-af2b-7a10d064210d.pdf

Data Driven Marketing Association. (2021). *How the Dutch think about data and privacy*. Retrieved from https://ddma.nl/privacy-monitor/

DeVore, G. R. (2017). Computing the z score and centiles for cross-sectional analysis: A practical approach. *Journal of Ultrasound in Medicine, 36*(3), 59–473. doi:10.7863/ultra.16.03025

Engbersen, G., van Bochove, M., de Boom, J., el Farisi, B., Krouwel, A., van Lindert, J., . . . van Wensveen, P. (2021). *De laag-vertrouwensamenleving: De maatschappelijke impact van COVID-19 in Amsterdam, Den Haag, Rotterdam & Nederland* [The low-trust society: The societal impact of COVID-19 in Amsterdam, The Hague, Rotterdam & the Netherlands]. Erasmus School of Social and Behavioural Sciences & Kenniswerkplaats Leefbare Wijken. Retrieved from https://www.impactcorona.nl/wp-content/uploads/2021/11/Def_-1-november_rapport_laag-vertrouwensamenleving_def83.pdf

Faia, M. A. (1980). The vagaries of the vignette world: A comment on Alves and Rossi. *American Journal of Sociology, 85*(4), 951–954. Retrieved from https://www.jstor.org/stable/2778714

Fiesler, C., & Proferes, N. (2018). "Participant" perceptions of Twitter research ethics. *Social Media + Society, 4*(1), 1–14. doi:10.1177/2056305118763366

Gilbert, S., Vitak, J., & Shilton, K. (2021). Measuring Americans' comfort with research uses of their social media data. *Social Media + Society, 7*(3), 1–13. doi:10.1177/20563051211033824

Goggin, B. (2019, January 6). Inside Facebook's suicide algorithm: Here's how the company uses artificial intelligence to predict your mental state from your posts. *Business Insider*. Retrieved from https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737–3757. Retrieved from https://ijoc.org/index.php/ijoc/article/view/4655/1738

Hicks, A. (2018). *Social democracy and welfare capitalism: A century of income security politics*. Ithaca, NY: Cornell University Press.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), Article 4. doi:10.5817/CP2016-4-7

Hox, J. J., Kreft, I. G. G., & Hermkens, P. L. J. (1991). The analysis of factorial surveys. *Sociological Methods & Research, 19*(4), 493–510. doi:10.1177/0049124191019004003

Huckins, G. (2020, December 14). An AI used Facebook data to predict mental illness. *WIRED*. Retrieved from https://www.wired.com/story/an-ai-used-facebook-data-to-predict-mental-illness/

Kantar. (2019). *The General Data Protection Regulation* (Special Eurobarometer Report 487a). European Commission. Retrieved from https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf

Krotoszynski, R. J. (2016). *Privacy revisited: A global perspective on the right to be left alone*. Oxford, UK: Oxford University Press.

Loohuos, K. (2020, April 24). Coronavirus: Dutch Covid-19 tracking app stirs national debate. *Computer Weekly*. Retrieved from https://www.computerweekly.com/news/252482131/Coronavirus-Dutch-Covid-19-tracking-app-stirs-national-debate

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society, 1*(2), 1–13. doi:10.1177/2053951714541861

Madden, M., & Rainie, L. (2015, May 20). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Martin, K., & Nissenbaum, H. (2020). What is it about location? *Berkeley Technology Law Journal, 35*(1)*,* 251–326. doi:10.2139/ssrn.3360409

Martin, K. E. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics, 111*(4), 519–539. doi:10.1007/s10551-012-1215-8

Maslowski, R. (2020). *"Onderwijs." De sociale staat van Nederland: 2020* ["Education." The social state of the Netherlands: 2020]. Sociaal Cultureel Planbureau. Retrieved from https://digitaal.scp.nl/ssn2020/onderwijs

Mols, A., & Janssen, S. (2017). Not interesting enough to be followed by the NSA. *Digital Journalism, 5*(3), 277–298. doi:10.1080/21670811.2016.1234938

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. doi:10.1177/0093650211418338

Pittman, M., & Sheehan, K. (2017). Ethics of using online commercial crowdsourcing sites for academic research. In M. Zimmer & K. Kinder-Kurlanda (Eds.), *Internet research ethics for the social age: New challenges, cases and contexts* (pp. 177–186). New York, NY: Peter Lang.

Rainie, L., Keeter, S., & Perrin, A. (2019, July 22). *Trust and distrust in America*. Pew Research Center. Retrieved from https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america/

Seltman, H. J. (2012). *Experimental design and analysis*. Pittsburgh, PA: Carnegie Mellon University.

Shvartzshnaider, Y., Tong, S., Wies, T., Kift, P., Nissenbaum, H., Subramanian, L., & Mittal, P. (2016). Learning privacy expectations by crowdsourcing contextual informational norms. In *Proceedings of the Fourth AAAI Conference on Human Computation and Crowdsourcing* (pp. 209–218). Menlo Park, CA: Association for the Advancement of Artificial Intelligence. doi:10.1609/hcomp.v4i1.13271

Smith, A. (2017, March 22). *What the public knows about cybersecurity*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

Strycharz, J., Ausloos, J., & Helberger, N. (2020). Data protection or data frustration? Individual perceptions and attitudes towards the GDPR. *European Data Protection Law Review, 6*(3), 407–421. doi:10.21552/edpl/2020/3/10

Trepte, S., & Masur, P. K. (2016). *Cultural differences in social media use, privacy, and self-disclosure*. University of Hohenheim. Retrieved from http://opus.uni-hohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf

Utz, C., Becker, S., Schnitzler, T., Farke, F. M., Herbert, F., Schaewitz, L., . . . Dürmuth, M. (2021). Apps against the spread: Privacy implications and user acceptance of COVID-19-related smartphone apps on three continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Article 70). New York, NY: ACM. doi:10.1145/3411764.3445517

Wagner, K. (2018, April 11). This is how Facebook uses your data for ad targeting. *Recode*. Retrieved from https://www.vox.com/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg

Wallander, L. (2009). 25 years of factorial surveys in sociology: A review. *Social Science Research, 38*(3), 505–520. doi:10.1016/j.ssresearch.2009.03.004

Xiao, Q. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy, 30*(1), 53–67. doi:10.1353/jod.2019.0004

Xu, H., Gupta, S, Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of the 33rd International Conference on Information System*s (pp. 2278–2293). Orlando, FL: Association for Information Systems.

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Chamberlain Kritikos, K. (2020). "There's nothing really they can do with this information": Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society, 23*(7), 1020–1037. doi:10.1080/1369118X.2018.1543442

Zureik, E., Harling Stalker, L., Smith, E., Lyon, D., & Chan, Y. E. (2010). *Surveillance, privacy and the globalization of personal information: International comparisons*. Montreal, Canada: McGill-Queen's University Press.