Abstract

Around the world, people increasingly generate data through their everyday activities. Much of this also happens unwittingly, thanks to sensors, cameras, and other surveillance tools on the roads, in cities, and in businesses. However, the ways citizens and governments think about privacy vary significantly around the world. In this paper, we explore differences between citizens' attitudes toward privacy and data collection practices in the U.S. and the Netherlands, an EU member nation. Using a factorial vignette survey methodology, we identify specific contextual factors associated with people's level of concern about how their data is being used. We consider the role that five factors play in this assessment: actors (those using data), data type and amount, reported purpose for data use, and inferences drawn from the data. These indicate nationally bound differences but likewise point to potentially more globally shared concerns.

Keywords: privacy, trust, data use, data practice, data collection, cross-cultural, GPDR

When Does Data Collection and Use Become a Matter of Concern?

A Cross Cultural Comparison of American and Dutch People's Privacy Attitudes

From posting on social media platforms to tracking sleep with a wearable device to simply using a smartphone, people increasingly generate data through their everyday activities. Much of this also happens unwittingly, thanks to sensors, cameras, and other surveillance tools on roads, in cities, and within businesses. As an example of the scope of this data generation, experts predict there will be more than 20 billion internet of things (IoT) devices like smart appliances operating worldwide in 2020 (Gartner, 2017).

The data generated throughout everyday life can provide important insights, both to individual users as well as 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 to predict and prevent future terrorist attacks; in the United States, the government has used national security as justification for intruding on individuals' privacy, as highlighted in Edward Snowden's revelations of mass government surveillance (Lyon, 2014), as well as the more recent court case between the FBI and Apple following a mass shooting in San Bernardino, California (Etzioni, 2018).

Technology adoption is widespread, especially among Western nations, and data collection and analysis for surveillance and usability purposes is common. However, the way citizens and governments think about privacy varies significantly around the world. One prominent example of cross-cultural differences in privacy is the comparison of European and American approaches. In 2016, the European Union (EU) passed the landmark General Data Protection Regulation (GDPR). This replaced its 1995 Data Protection Directive, which already

extended significant privacy rights to citizens, to account for the vast technological advances in data collection practices during the 21st century (Safari, 2016). Specifically, the GDPR gives EU citizens more control over their data and creates new restrictions and reporting requirements for companies that collect data from citizens (Bremmer, 2018). The GDPR also extended Europe's "right to be forgotten" court ruling from 2014 that gave citizens additional rights to control the visibility of information about them on search engines (Mantelero, 2013). These regulations differ significantly from approaches the U.S., which has yet to pass federal legislation on privacy, instead relying on a mishmash of torts, sector-specific federal laws, and state laws (Schryver, 2019).

In this paper, we explore differences between citizens' attitudes toward privacy and data collection practices in the U.S. and the Netherlands, an EU member nation. Using a factorial vignette survey methodology (Wallander 2009), we identify specific contextual factors associated with people's level of concern about how their data is being used. We consider the role that five factors play in this assessment: actors (those using data), data type and amount, reported purpose for data use, and inferences drawn from the data. In our analyses, we address the following research questions:

RQ1: How do trust and privacy-related attitudes toward data use vary across American and Dutch people?

RQ2: What are the differences/similarities between Americans and Dutch in their data use concern based on contextual factors?

Findings from our analyses highlight both similarities and discrepancies in how citizens of the two nations evaluate the privacy risks of different data practices. We conclude the paper by noting that American and Dutch respondents differ in the kinds of personal data and the

inference they may produce that shape their concerns. However, they are also aligned in a way that may point to potential global privacy fears - including concern regarding the predominance of American platforms - that transcend borders and boundaries.

Background

As digital technologies become increasingly embedded into everyday life, they introduce new flows of information that shift boundaries and challenge entrenched privacy norms and expectations. For example, the Cambridge Analytica scandal in early 2018 spotlighted how data collected from one's social network activities might be used for psychometric profiling of political motivations (Cadwalladr & Graham-Harrison, 2018). In another example, apps used to help track one's mood or menstrual cycles might unexpectedly share users' sensitive data with third parties (Becker, 2019). Such challenges of managing personal information flows in our contemporary information ecosystem are encapsulated in Marwick & boyd's (2014) concept of "networked privacy," defined as the "ongoing negotiation of contexts in a networked ecosystem in which contexts regularly blur and collapse" (p. 1063).

These challenges of negotiating privacy within and across networked contexts is central to Nissenbaum's (2010) theory of contextual integrity (CI). CI takes context as its starting point, arguing that all our data and technological interactions occur in particular contexts, and that informational norms govern people's expectations of how personal data should flow within a given context. Researchers across numerous disciplines have applied CI to various cases where new technologies appear to impact norms of information flows, such as search engines (Zimmer, 2008), social media platforms (Shi, Xu, & Chen, 2013), location-based technologies (Barkhuus, 2012), electronic medical records (Chen & Xu, 2014), and smart home devices (Apthorpe,

Shvartzshnaider, Mathur, Reisman, & Feamster, 2018), among others. Across such studies, researchers have identified nuanced explanations for perceived "inconsistencies" or "paradoxes" in privacy behaviors, suggesting that breaches in contextual integrity can help explain why users would be concerned about uses of data that go beyond the original purpose or context in which they were initially generated.

Our work is motivated by the nuance a more contextual approach to privacy empowers. Through the factorial vignette approach (described below), we seek to isolate how users might consider the appropriateness of data collection and use across multiple variables and contexts. More importantly, we seek to understand how such contextual attitudes might also differ across cultures, focusing on the United States and the Netherlands. The differences between legal and regulatory approaches to privacy within the United States versus the European Union have been well documented and analyzed (Bennett & Raab, 2006; Schwartz & Solove, 2014; Krotoszynski, 2016). We seek to build on this recognition to determine if cultural differences in privacy attitudes and behaviors regarding contextual appropriateness of data use are discoverable across U.S. and Dutch populations.

Privacy Attitudes and Behaviors in the U.S. Context

A significant amount of research has explored the digital privacy attitudes, knowledge, and behaviors of Americans. Looking at national trends of U.S. adults, Pew Internet has found that Americans overwhelmingly think it is important they have control over what data is collected about them and who can access their data; at the same time, however, they have little confidence that the government and companies can effectively protect their data (Madden & Rainie, 2015). Furthermore, results from a 13-item Pew "cybersecurity quiz" revealed that most Americans have limited knowledge of cybersecurity concepts and practices, with the average

respondent answering just 5.5 questions correctly (Smith, 2017). Numerous studies have highlighted that Americans have low digital literacy skills, especially as it relates to the increasingly complex task of protecting personal data (see, for example, Park 2013).

With the emergence and popularity of social media platforms, researchers began focusing on the privacy implications of sharing personal information in (semi-) public spaces. One of the most dominant streams of research has used the "privacy paradox" to frame the discrepancy between internet users' stated privacy concerns and their sharing patterns. Early research in this space—often looking American college students—found that young people said they had privacy concerns but shared significant amounts of information on sites like Facebook (e.g., Acquisti & Gross, 2006; Barnes, 2006). In more recent years, however, researchers have begun to understand this negotiation between privacy and disclosure to be more nuanced and depend on perceived benefits and risks, as well as a number of contextual factors (e.g., Baruh, Secinti, & Cemalcilar, 2017; Shi, Xu, & Chen, 2013).

Privacy attitudes in the U.S. are also likely influenced by the presence of most of the world's largest technology companies as well as the country's policies regulating individual privacy rights. The rise of big data analytics—and the ease with which companies and individuals can now collect and analyze end-user data—has raised numerous concerns about the rights individuals have over their data, highlighting the inherent limits of "anonymity" and "consent" in the 21st century (Barocas & Nissenbaum, 2014). Many researchers have highlighted that Americans have developed a sense of apathy (Hargittai & Marwick, 2016), cynicism (Hofffam, Lutz, & Ranzini, 2016), or resignation (Turow, Hennessy, & Draper, 2015) toward privacy protections in the face of the Edward Snowden revelations, frequent data breaches, and general lack of protections in place.

Privacy Attitudes and Behaviors in the Dutch Context

Media coverage may frame GDPR as a struggle between Silicon Valley and Brussels (Bode, 2018), yet this oversimplifies the relationship between these spheres of influence as well as the attitudes and repertoires of American and Dutch people. To some degree, it is possible to consider the Netherlands as an approximation of broader idealized 'European' attitudes toward privacy. As one of the six founding members of the EU, its population reports a comparatively strong understanding of European legal mechanisms that have recently been implemented to protect privacy. In a recent Eurobarometer survey, 87% of Dutch respondents heard about the GDPR, and 60% claim they know what it is—ranking second highest of all 28 European countries in the survey (Kantar, 2019). Dutch respondents score highest on awareness of the right to be forgotten, the right to access data, the right to correct data, and the right to object to receiving direct marketing. Moreover, with 82% of the respondents being aware of the existence of a national public data protection authority, the awareness of the GDPR, specific rights and the bodies to protect these rights are high, especially compared to other EU countries (Kantar, 2019).

Dutch attitudes towards privacy and institutional trust are shaped by their recent socio-political context, including the absence of authoritarian regimes found in other EU member states like Spain and Hungary (Zureik et al., 2010). Beyond a lack of authoritarianism, Dutch trust in institutions is arguably also shaped by the so-called "polder model," with the necessity for otherwise-siloed religious and political interest groups needing to seek consensus when forming governments (den Butter and Mosch, 2003). Yet relative trust in governments does not preclude a responsibilization of privacy management among the Dutch. A market-initiated report about privacy attitudes indicates that one-quarter of Dutch citizens feel they are responsible for their data protection, 23% believe this is a task of the government, and only 3% puts this in the hands

of companies, whereas 40% believes in a combination of the options provided (DDMA, 2018). In terms of taking steps to preserve privacy online, a recent study suggests that Dutch users balance a lack of confidence in their own abilities to protect their privacy with some confidence in the range of protective behaviors available (Boerman et al., 2018).

The relative novelty of information and communication technologies implies a perceived need to come to terms with privacy threats alongside privacy remedies. A survey from the Dutch Data Protection Authority (Autoriteit Persoongegevens, 2019) found respondents were most concerned about (copies of) their ID card (85%), closely followed by online search history (82%), mobile location data (80%), social media messages and images (75%), social identification number (73%), and log-in details to government services (73%). Less concern was raised by financial data (66%), medical data (65%), municipality registration data (53%), debts/criminal records (57%), camera footage (56%), and finally, children's education records (47%). This suggests a heightened concern for data most typically associated with smartphones (browsing, location, messaging). However, online banking and sensitive data from governments (e.g., through the government services 'MijnOverheid' app) also suggests that concern for any single type of personal data increasingly implies concern for mobile and other novel forms of data handling.

In the following section, we describe how we created and distributed our survey study to adults in the U.S. and the Netherlands before presenting findings comparing privacy attitudes across the two countries.

Method

Factorial Vignette Survey: An Experimental Design

The situational similarities and differences between the two countries and the complexities inherent in privacy attitudes, particularly in relation to mobile data, led us to pursue more innovative approaches to understand cultural variations in privacy attitudes. We draw on the factorial vignette survey method, which provides a bridge between experiments and surveys (Wallander, 2009). Rossi and colleagues (1979) pioneered the factorial survey approach, which includes the use of classical experimental designs in the context of broadly based sample surveys. Their vignette techniques typically entail short descriptions of scenarios in which the characteristics presumed to be relevant to some outcome are systematically varied. Each vignette is followed by at least one rating task where respondents indicate their judgments.

This methodology is well-suited for studying nuanced social phenomena. Since changes in the vignettes are subtle, respondents are less susceptible to social desirability bias seen in conventional surveys (Wallander, 2009; Taylor, 2006). Compared to traditional survey research, factorial vignette surveys avoid non-orthogonal or collinear factors that occur in association with each other. The random combination of factors "ensures any non-orthogonality of the independent variables is due to random error only" (Taylor, 2006, p. 1197).

Factorial vignette surveys are frequently used in research on complex judgments and beliefs in a variety of contexts, such as the norm of political action (Jasso & Opp, 1997), end-of-life medical decisions (Han et al., 2016), and immigration issues (Short & Magaña, 2002). Martin (2012) used the factorial vignette survey method to evaluate privacy norms. We build on her work and apply this method to study cross-cultural differences in privacy norms.

Constructing vignettes. Vignettes are hypothetical scenarios with varying factors. In each vignette, the factors are altered slightly, and the respondent is asked to evaluate each unique scenario. As a simple example, a survey about information disclosure norms could vary the

factors of role (e.g., boss, bus driver) and information type (birthday, sexual orientation), yielding four vignettes. Respondents would then be asked to evaluate whether it would be appropriate to ask for their boss's birthday, their boss's sexual orientation, their bus driver's birthday, and their bus driver's sexual orientation. Below, we describe how we identified factors, created vignettes, and developed the survey.

Vignette factors. Our construction of vignettes was guided by Nissenbaum's (2010) contextual integrity framework. Based on the framework, we identified five factors relevant to people's interpretations of privacy norms: Actor (who is using the data), Content/Information Type (what kind of data is being used), Amount (how much data), Inference (what data reveal), Purpose (why the data are used). Within each factor, there are different levels that are purported to influence respondents' privacy judgment and expectation. Figure 1 shows a sample vignette as it appeared to respondents. Table 1 lists the levels measured for each factor.

--FIGURE 1 & TABLE 1 ABOUT HERE--

Narrowing the vignette universe. The initial vignette universe included 6912 possible combinations: 6(Actor) x 8(Content) x 3(Amount) x 6(Inference) x 8(Purpose). Prior work recommends deleting vignettes that depict unrealistic 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). Rossi (1979) also insisted that authors of factorial survey studies pay continuous attention to the realism of their results. Heeding this call, the lead author identified unrealistic scenarios, such as "Your doctor (Actor) using data for Improving traffic flow in your region (Purpose)." The full team reviewed the list of unrealistic scenarios and discussed them, resolving

disagreements through consensus. Our final vignette universe included 5232 combinations. These vignette texts were generated automatically using Python scripts and then uploaded to Qualtrics, an online survey platform.

Vignette survey. Each vignette was accompanied by two statements: "This use of my data is appropriate" and "This use of my data would concern me." For each vignette, respondents were asked to rate their level of agreement with the two statements. (See Figure 1 for a screenshot of how the vignettes appeared to respondents).The survey was developed in English and translated into Dutch.

Data collection. Survey data was collected in May 2019. U.S. respondents were recruited from Amazon Mechanical Turk, while Dutch respondents through IPSOS. The Dutch sample is representative of the Dutch population, while the American sample is not. Each respondent was given 32 vignettes randomly selected with replacement from the 5232 vignettes. Ninety-three percent of respondents completed all 32 vignettes. After removing incomplete and low-quality responses, the final dataset included 10,433 vignette responses from 329 American respondents and 14,588 responses from 511 Dutch respondents.

Measures

Dependent variables (DVs). The survey measured two dimensions of privacy judgment along a five-point, Likert-type scale (1=Strongly Disagree—5=Strongly Agree): **Data Use Concern,** American: M=4.20, SD=1.07, Dutch: M=3.95, SD=1.20, and **Perceived Appropriateness of Data Use**, American: M=1.70, SD=1.00, Dutch: M=1.72, SD=1.01. After reading each vignette, respondents were asked to rate their level of agreement with two statements: 1) This use of my data would concern me, and 2) This use of my data is appropriate (see Figure 1). For Data Use Concern, a higher value indicates the respondent perceives greater

data privacy concerns associated with the presented scenario. For Appropriateness of Data Use, a higher value indicates the respondent felt the data use was 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 paper, we only report findings from analyses using Data Use Concern as the DV. The first reason is to avoid redundancy. Based on initial mixed effect modeling using the American sample, we found significant factors echoed in both models with the opposite effect on levels of data use concern and perceived appropriateness. Additionally, since the word "appropriate" does not have a direct translation in Dutch, we used the alternative Dutch word *"gerechtvaardigd"* which emphasizes the legality rather than norm. We chose to focus on Data Use Concern to make cross-cultural comparative analyses more robust and reliable.

Dimensions of vignette factors. The primary explanatory variables in this study are the privacy factors that constitute the vignettes: Actor, Content, Amount, Inference, Purpose.

Trust toward social institutions (American: M= 2.52, SD=.96, α=.88, Dutch: M=2.80, SD=.89, α=.89). We used a five-point Likert scale to measure respondents' trust toward social institutions based on how much they agreed or disagreed with the following statements: 1) Most of the time I trust people in my local government to do what is right; 2) Most of the time I trust American companies[1] to do what is best for consumers; 3) Most of the time I trust the social media platform (that I use the most) to do what is best for consumers; and 4) Most of the time I trust the news media to do what is right in their reporting. Response options ranged from 1 (Strongly Disagree) to 5 (Strongly Agree).

[1] Note that given the prevalence of American companies (e.g., Apple, Google, Facebook, etc.) in mobile activities Dutch respondents were also asked about their trust in American companies.

Mobile privacy concern (Xu et al., 2012; American: *M*=3.95, *SD*=.65, *α*=.91, Dutch: *M*=3.89, *SD*=.70, *α*=.92). Respondents were asked to rate their level of agreement with eight statements, including: "I am concerned that mobile apps are collecting too much information about me." and "I am concerned that mobile apps may monitor my activities on my mobile device." Each item was recorded from 1 (Strongly Disagree) to 5 (Strongly Agree), with a higher value indicating a higher level of mobile privacy concern.

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

*Privacy resignation/fatalism (*American: *M*=2.41, *SD*=.75, *α* =.74, Dutch: *M=2*.88, *SD*=.68, *α*=.80). Resignation was measured using a four-item scale based on respondents' level of agreement with the following statements: 1) There is nothing I can do to protect my privacy and security online, 2) In the online world, privacy does not exist anymore, 3) There's nothing I can do to prevent my account from being hacked, and 4) I don't have control over the information I share online. Participant responses were recorded on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

Privacy pragmatism (American: M=2.47, *SD*=1.06, *α* =.79, Dutch: *M=2.63*, *SD*=1.04, *α*=.84). Pragmatism was measured using two-item scale based on the level of agreement with the statements: 1) "I might trade my personal data for convenience" and 2) "I might give my

personal data for a reduced cost of service." Participant responses were recorded on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

Control variables. We also included several control variables.

- Age: The American sample has an average age of 36.45 years old *(SD*=10.52), with a range from 18 to 72 years old. The Dutch sample has an average age of 46.13 (*SD*=14.16) years old, with a range from 18 to 66 years old.
- Education: Among U.S. respondents, 32.1% of respondents had less than a bachelor's degree, 54.6% obtained a bachelor's degree, and 12.7% received a postgraduate degree. On the Dutch side, the rates are 21.2%, 41.2%, and 37.6%, respectively.
- Sex*:* 60% of American respondents were male; 49% of Dutch respondents were male.

Data Analysis

We used a combination of R, particularly, lme4 package, and SPSS to perform data analysis. To answer RQ1, we conducted independent sample t-tests to uncover differences between American and Dutch consumers in their level of trust, mobile privacy concerns, and privacy-related beliefs including pragmatism and resignation/fatalism.

Our factorial survey sampled both respondents and vignettes. Therefore, the data was generated in two distinct levels: the individual level and the vignette level. To accommodate the hierarchical structure of this dataset, we used mixed effect modeling to account for within- and between-subjects differences (Hox, 1991). It is important to note that all vignette- and respondent-level variables can possibly modify the judgment threshold. Therefore, in the final models, we included both individual characteristics (e.g., age, trust, privacy beliefs) and vignette factors 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 concerns based on the type of actors, content, amount, inference, and purpose of data use. However, American respondents generally reported higher concerned across all types of vignette factors. With such differences in the threshold of judgment, we need to go beyond the simplistic comparison between the absolute value of means. Therefore, we calculated the z-scores for more meaningful cross-cultural comparative analyses. As a classical method of data normalization, z-score transformation provides a way of standardizing data across a wide range of experimental conditions and allows the comparison of data independent of the original propensity (Devore, 2017; Cheadle et al, 2003).

Results

Evaluating American and Dutch People's Differences in Trust and Privacy Beliefs

The vignette survey asked a series of questions to evaluate people's existing beliefs related to trust and privacy in order to analyze the similarities and differences between American and Dutch respondents.

Differences in level of mobile privacy concerns. Both sampled populations reported a relatively high degree of mobile privacy concerns, with each item scoring around four out of five points. Compared to the Dutch, Americans generally reported higher levels of privacy concerns related to their mobile app use. These differences for each item evaluating mobile privacy concerns were statistically significant, except for items 3, 6, and 8. Details of itemized means and t-test results are shown in Table 2.

--TABLE 2 ABOUT HERE --

Differences in level of trust in social institutions. Compared to the Dutch sample, Americans reported statistically significant lower levels of trust in federal government, $t(819)$=-

6.33, $p<.001$, local government, $t(819)=-3.6$, $p<.001$, social media platforms, $t(819)=-4.75$, $p<.001$, and the news media, $t(819)=-4.14$, $p<.001$. Details of itemized means and t-test results are shown in Table 3. There was no significant difference in the trust in American companies—both American and Dutch respondents indicated similarly low trust in American companies.

--TABLE 3 ABOUT HERE --

Differences in the degree of resignation/fatalism. Compared to the American sample, Dutch respondents reported a statistically higher degree of resignation/fatalism related to online privacy. Specifically, they were more inclined to agree with these statements: "There is nothing I can do to protect my privacy and security online," $t(820)=-6.12$, $p<.001$; "In the online world, privacy does not exist anymore," $t(820)=-8.33$, $p<.001$; "There's nothing I can do to prevent my account from being hacked," $t(820)=-9.12$, $p<.001$; and "I have no control over the information I share online," $t(820)=-5.6$, $p<.001$. Details of itemized means and t-test results are shown in Table 4.

--TABLE 4 ABOUT HERE --

Differences in degree of privacy pragmatism. Compared to American respondents, the Dutch reported a higher degree of pragmatism related to online privacy. They were more willing to trade their data for convenience, $t(819)=-7.54$, $p<.001$, or a reduced cost of service, $t(819)=-13.81$, $p<.001$) Details of itemized means and t-test results are shown in Table 5.

--TABLE 5 ABOUT HERE--

Explaining Data Use Concerns: Difference And Similarities

As shown in Table 6, 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 ANOVA, or ANCOVA depending on the nature of these explanatory variables (Seltman, 2012).

--TABLE 6 ABOUT HERE--

Cross-country comparison: Roles of individual characteristics. Table 7 presents more detailed model results to unpack how individual characteristics might shape consumer concerns about data use. We offer interpretations that focus on comparing similarities and differences between the American and Dutch samples. Specifically, we examine variables that are statistically significant and how much (i.e., standardized coefficient) they weigh on the respondents' data use concerns.

--TABLE 7 ABOUT HERE--

The patterns of individual characteristics that influence data use concerns are quite similar among Dutch and American respondents. In both groups, older respondents and those who expressed a higher level of mobile privacy concerns were more likely to consider a data use scenario concerning (β_A=.01, p<.05; β_D=.01, *p*<.05). People who reported higher levels of fatalism appeared to be less concerned about data use (β_A=.-11, p<.001; β_D=-.25, *p*<.001). Education, gender, and self-efficacy were not significant in either sample.

The differences regarding the effects of individual characteristics manifest in the level of trust (β_A=.-09, *p*<.05) and pragmatism belief (β_A=.-09, *p*<.05), both of which were statistically significant in the American sample but not in the Dutch sample. Additionally, mobile privacy concerns had a larger effect among American respondents (β_A=.54, p<.001; β_D=.37, *p*<.001), while a sense of fatalism had a larger effect among Dutch (β_A=.-11, p<.001; β_D=-.25, *p*<.001).

Cross-country comparison: Roles of data use context. Respondents' concerns about data use varied by vignette attributes. Table 8 lists the effects (i.e., estimated coefficient) of each

dimension of vignette factors on the level of data use concern (DV). Note that these effects should be interpreted using a reference level within each type of vignette factor.

--TABLE 8 ABOUT HERE--

In order to directly differentiate the levels of concern across the American and Dutch populations, 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 factors while adjusting for other covariates (e.g., age and mobile privacy concerns) and the random effects.

Effects of actor types on data use concern. The overall models (see Table 8) show that there were significant effects of actor type on data use concerns for both samples [American: ($F(5,9992)=7.68$, $p<.001$), Dutch: ($F(5,12415)=45.84$, $p<.001$)]. Figure 2 presents the pairwise comparison results with the estimated mean of concerns for six types of actors: online data broker, social media (most frequently used), law enforcement, company's HR department, doctor, and local government.

-- FIGURE 2 ABOUT HERE --

Compared to the Dutch sample, American respondents generally had higher concerns across all types of actors. To account for the different thresholds of concern between two sampled populations, we normalized the mean values and calculated z-scores to reflect the *actual fluctuations* in levels of concern based on different actor types. Figure 3 shows z scores for normalized data concern values across actor types. 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 that actor's use of data.

-- FIGURE 3 ABOUT HERE --

Dutch respondents reported a lower level of data use concern when the actors were local government and law enforcement. To the contrary, Americans felt more concerned about data use by these two actors. Both American and Dutch respondents expressed higher concerns 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 to Americans. Both American and Dutch respondents felt less concerned about data use by their doctor and social media, but the degrees of concern are much lower among Americans.

Effects of content types on data use concern. The effect of content type on the level of concern was statistically significant among American respondents, $F(7,10008)=15.00$, $p<.001$. However, for the Dutch sample, such an effect was not statistically significant, $F(7,12425)=45.84$, $p=0.8$. Figure 4 presents pairwise comparison results with the estimated mean of concerns based on eight types of content.

-- FIGURE 4 ABOUT HERE --

Using the normalized values, we compared the two samples and identified several similarities and differences. Figure 5 shows standardized z-scores of data concern based on types of content. Dutch respondents were less concerned about the use of web browsing search history, while Americans were more concerned about it. Both Dutch and American respondents became more concerned about data use related to their text-based posts and messages, photos and video posts, phone call log data, and emails. However, the Dutch were significantly more concerned about their photos and video posts compared to Americans, while Americans were more concerned about their emails compared to the Dutch. Conversely, both samples were less concerned about social media posts, physical activity data, and phone call log data. But

Americans appeared to care much less about physical activity data and more about their social media posts compared to the Dutch.

-- FIGURE 5 ABOUT HERE --

Effects of amount on data use concern. The effect of data amount was statistically significant for the American respondents, $F(2, 10007)=20.78$, $p<.001$, but not for the Dutch, $F(2,12424)=.60$, $p>0.05$. Figure 6 presents pairwise comparison results with the estimated mean of concerns based on amount of data.

-- FIGURE 6 ABOUT HERE –

Figure 7 shows standardized z-scores based on amount of data used. Both American and Dutch respondents expressed less concern about one week's worth of data being used, but more concern about one year's worth of data or the full history of data.

-- FIGURE 7 ABOUT HERE --

Effects of inference types on data use concern. The effects of inference on data use concerns were statistically significant for both samples [American: ($F(5,10009)=19.23$, $p<.001$), Dutch: ($F(5,12415)=13.15$, $p<.001$)]. Figure 8 presents pairwise comparison results with the estimated mean of concerns based on six inferences.

-- FIGURE 8 ABOUT HERE --

Figure 9 shows standardized z-scores based on types of inference. We found more similarities than differences in the ways American and Dutch respondents reacted to various data inferences. The only cross-cultural difference observed was the inference of mental state. Americans felt more concerned when data were used to infer their mental state, while the Dutch felt less concerned. Otherwise, both American and Dutch felt more concerned when data were used to infer their sexual orientation, political views, and the friend network. Conversely, both

samples felt less concerned when data were used to infer places that they visited and how healthy they were, although Americans were significantly less concerned about the inference of how healthy they are.

-- FIGURE 9 ABOUT HERE --

Effects of purpose types on data use concern. The effects of purpose on data use concerns were statistically significant for both samples [American: $F(5,10009)=19.12$, $p<.001$; Dutch: $F(5,12415)=17.98$, $p<.001$]. Figure 10 presents pairwise comparison results with the estimated mean of concerns based on eight purposes.

-- FIGURE 10 ABOUT HERE --

Taking the normalized values into consideration, we observe several differences in the ways American and Dutch respondents reacted to various data use purposes. Figure 11 shows standardized z-scores based on purposes. Dutch respondents were less concerned about data use for two public safety-related purposes: 1) preventing or reducing criminal activity, and 2) fighting terrorism. However, Americans considered these two purposes more concerning. The Dutch were more concerned about the purposes of 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 American and Dutch respondents expressed higher concerns when data were collected for the purpose of providing personalized advertising and creating a national database for citizens. And both samples became less concerned about data use for the purpose of improving traffic flow in the region.

-- FIGURE 11 ABOUT HERE --

Discussion

Through a factorial vignette survey conducted in the U.S. and the Netherlands, we explored cross-cultural variations in people's trust, privacy attitudes, and data use concern across a variety of contextual factors. Such evaluations are increasingly important to consider as different countries respond to advances in information and communication technologies by taking varied approaches to defining basic privacy rights and protecting citizens' data.

Our first set of analyses compared American and Dutch respondents' trust and privacy-related attitudes. With regard to trust toward social institutions which arguably both regulate and make use of (personal) data, analyses revealed a cross-cultural difference in the level of trust toward the government; Dutch respondents placed a higher level of trust in their government than Americans. This higher trust in government might associate with the stronger presence of Dutch government in the public sphere, as demonstrated by the government-initiated welfare policies in the Netherlands (Hicks, 2018). Americans' lower trust in the government aligns with a trend of declining trust (Rainie, Keeter, & Perrin, 2019) and disapproval of government intervention. Both American and Dutch respondents expressed low trust in American companies to do what is best for consumers. This finding is not surprising given the recent Cambridge Analytica scandal and other instances related to privacy violations.

Additionally, we identified how American and Dutch respondents differed in their privacy-related attitudes. Compared to Americans, Dutch respondents expressed lower level of privacy concerns, which might be explained by their higher level of resignation and pragmatism beliefs alongside the belief that levels of government, in particular the EU, would intervene in particularly egregious privacy violations. Specifically, Dutch respondents were more likely to agree with statements indicating a resignation related to privacy, such as "There is nothing I can do to protect my privacy and security online" and "I have no control over the information I share

online." Likewise, Dutch respondents were more likely to agree with statements indicating their pragmatic approach to personal data, such as "I might trade my personal data for convenience" and "I might give my personal data for a reduced cost of service."

Furthermore, we constructed two mixed-effect models to explain how people's data use concern was shaped by both individual characteristics and contextual factors. According to the models, the effects of individual characteristics are similar across American and Dutch respondents. Data use concern was positively correlated to participant age and mobile privacy concerns, and negatively correlated with resignation and pragmatism beliefs.

Beyond individual characteristics, the models also revealed how five types of contextual factors influenced data use concerns. We further conducted comparative analyses using the normalized values of data use concerns for each type of factors across the Dutch and American respondents. In terms of the effects of actor, the most striking difference lay at the shifting of data use concerns when the government was involved. When holding the other factors constant, the presence of local government seemed to have decreased Dutch respondents' but increased Americans' concerns. The same contrast occurred when the actor was law enforcement.

Another set of major cross-cultural differences were observed when considering different purposes of data use. The Dutch became more concerned—and Americans less concerned—when data were used for the purpose of reducing 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/GPs as most trustworthy with personal information at 66% (DDMA, 2018), a separate study reports that insurance companies (together with banks) are among the most troubling organizations when it comes to misuse of personal data (Autoriteit Persoongegevens,

2019). Alternatively, the relative lack of concern with binge drinking in the Dutch context may also explain why they object to collecting personal data for this cause.

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. The heightened concern among Americans might be associated with disapproval of government surveillance post-Snowden revelations; Americans broadly found it unacceptable for the government to monitor U.S. citizens (PEW, 2015). Conversely, Dutch public discourse finds critical framings coexisting with more accepting attitudes towards surveillance in the post-Snowden context (Mols & Janssen, 2017). This might also be connected to the Dutch orientation to pragmatism, which in this case would anticipate that governments have to work within certain regulatory boundaries. As such, within legal limits, the use of data for safety and security may be seen as expected and accepted.

Despite the variations in how Dutch and America respondents felt about different actors and data use purposes, we observed similar trends in their attitudes for the remaining three factors-- content, amount and inference. For example, both samples felt less concerned when only one week's worth of data were used. There were only two exceptions related to content and inference, respectively. Dutch respondents were less concerned about the use of web browsing search history, while Americans were more concerned about such use. Dutch respondents were less concerned about data used to infer mental state, but Americans grew more concerned.

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, yet both American and Dutch respondents share distrust in American companies. We also observed divergence in

attitudes towards purposes of data use, with the Dutch having more concern with public health initiatives, and Americans being more opposed to the use of personal data for combating crime and terrorism.

Study strengths and limitations. The current study offers a novel methodology to explore the contextual factors that influence people's privacy-related judgment. As a bridge between experiments and surveys (Wallander, 2009), the factorial vignette survey methodology carries the strengths and weaknesses of both types of empirical work (Martin, 2012). The highly controlled nature of the vignettes ensures greater internal validity than in usual surveys. Since a large number of contexts affecting privacy judgments are systematically varied (Taylor, 2006), the methodology captures the complexities of privacy related norms and decision-making. In addition, since changes in the vignettes are subtle, respondents are less susceptible to social desirability bias as in conventional surveys (Wallander, 2009; Taylor, 2006).

However, in the analysis, pervasive cultural or personality differences may also explain the variances between contracting groups' responses (Martin, 2012). We tried to mitigate these incongruences by using mixed-effects modeling to account for individual differences within each group. Another limitation originated in the initial vignette construction, where researcher bias can influence the inclusion of factors, and missing factors could change the final models for each group. As noted above, the differences in representativeness of the samples may have implications as to the degree of comparability between the American and Dutch data. Finally, the results point to the attitudes of the respondents rather than their expected behavior. Future research would benefit from qualitative data to unpack the findings from our study.

Conclusion

While information and communication technologies are increasingly borderless, how countries regulate companies and protect citizens' data varies significantly. In this paper, we compared citizens' privacy concerns regarding data use in two very different regulatory contexts—the U.S. and the Netherlands (part of 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.

The findings suggest that 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--may help reduce some of their concerns. While the U.S. does not yet have comprehensive privacy legislation, California will enact legislation similar to GDPR (California Consumer Privacy Act of CCPA) in 2020. This change will provide important insights into what federal regulations might look like. However, while some personal concerns may be mitigated by such legislation, the potential association at least in this study between higher levels of resignation and trust in government indicate an increased responsibilization that shifts away from both users and companies gathering data. For many this may be normatively desirable, but we need to recognize this as a political choice with socio-economic implications.

References

Acquisti, A. and R. Gross (2006). *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook,* Springer Berlin / Heidelberg.

Anonymous. (2016, June 16). The history of the European Union. Retrieved October 29, 2019, from European Union website: https://europa.eu/european-union/about-eu/history_en

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering IoT smart home privacy norms using contextual integrity. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* (Vol. 2, 2).

Autoriteit Persoonsgegevens. (2019). Nederland maakt zich zorgen over privacy [Flitspeiling privacyrechten]. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/resultaten_enquete_privacyzorgen_jan_2019.pdf.

Barnes, S. B. (2006). "A privacy paradox: Social networking in the United States." First Monday 11(9), n.p.

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM*, 57(11), 31-33.

Barkhuus, L. (2012). The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 367–376). Austin, TX.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67, 26-53. https://doi.org/10.1111/jcom.12276

Becker, R. (2019, April 20). That mental health app might share your data without telling you. *The Verge.* Available: https://www.theverge.com/2019/4/20/18508382/apps-mental-health-smoking-cessation-data-sharing-privacy-facebook-google-advertising

Bode, K. (2018, May 25). What is GDPR and What Can America Learn From it? Vice.com. Retreived from https://www.vice.com/en_us/article/xwmx3n/what-is-gdpr

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research* (online first).

Bremmer, I. (2018, May 25). Europe's New Privacy Law Takes Effect Today. Here's How the World Is Handling Digital Rights. Time Magazine. Available: https://time.com/5291529/gdpr-digital-privacy/

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

Cheadle, C., Vawter, M. P., Freed, W. J., & Becker, K. G. (2003). Analysis of Microarray Data Using Z Score Transformation. *The Journal of Molecular Diagnostics*, 5(2), 73–81. https://doi.org/10.1016/S1525-1578(10)60455-2

Chen, Y., & Xu, H. (2013). Privacy management in dynamic groups: understanding information privacy in medical practices. In *Proceedings of the 2013 conference on Computer supported cooperative work (CSCW '13)* (pp. 541-552), New York, NY, USA: ACM.

Data Driven Marketing Association. (2018). DDMA Privacy Monitor: Wat Consumenten Denken. Retrieved from https://ddma.nl/download/66878/

Den Butter, F. A., & Mosch, R. H. (2003). The Dutch miracle: Institutions, networks, and trust. *Journal of Institutional and Theoretical Economics JITE*, 159(2), 362-391.

DeVore, G. R. (2017). Computing the Z Score and Centiles for Cross-sectional Analysis: A Practical Approach. *Journal of Ultrasound in Medicine,* 36(3), 459–473. https://doi.org/10.7863/ultra.16.03025

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in‐depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, 45(3), 285-297.

Etzioni, A. (2018). Apple: Good business, poor citizen?. *Journal of Business Ethics*, 151(1), 1-11.

Gartner. (2017, February 7). Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Han, P. K. J., Dieckmann, N. F., Holt, C., Gutheil, C., & Peters, E. (2016). Factors Affecting Physicians' Intentions to Communicate Personalized Prognostic Information to Cancer Patients at the End of Life: An Experimental Vignette Study. Medical Decision Making: An International Journal of the Society for Medical Decision Making, 36(6), 703–713. https://doi.org/10.1177/0272989X16638321

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. International Journal of Communication, 10, 21.

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

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal*

Jasso and Opp. (1997). *Probing the Character of Norms: A Factorial Survey*. Retrieved from https://www.researchgate.net/profile/Karl_Dieter_Opp/publication/271807765_Probing_the_Character_of_Norms_A_Factorial_Survey_Analysis_of_the_Norms_of_Political_Action/links/54dc85fa0cf25b09b91221a8.pdf

Jasso, G., & Opp, K.-D. (1997). Probing the Character of Norms: A Factorial Survey Analysis of the Norms of Political Action. American Sociological Review, 62(6), 947. https://doi.org/10.2307/2657349

Kantar. (2019). *The General Data Protection Regulation* (Special Eurobarometer Report 487a:). European Commission. Retrieved from https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. Big Data & Society, 1(2), 1-8. doi:0.1177/2053951714541861

Madden, M., & Rainie, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. Pew Internet Project. Available: https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. Computer Law & Security Review, 29(3), 229-235.

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. https://doi.org/10.1007/s10551-012-1215-8

Mols, A., & Janssen, S. (2017). Not Interesting Enough to be Followed by the NSA: An analysis of Dutch privacy attitudes. *Digital Journalism* 5(3), 277-298.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215-236.

Rainie, L., & Madden, M. (2015, March 16). *Americans' Privacy Strategies Post-Snowden.* Retrieved October 29, 2019, from Pew Research Center: Internet, Science & Tech website: https://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Rainie, L., Keeter, S., & Perrin, A. (2019). *Trust and Distrust in America*. Pew Research Center. Available: https://www.people-press.org/2019/07/22/trust-and-distrust-in-america/

Safari, B. A. (2016). Intangible privacy rights: How europe's gdpr will set a new global standard for personal data protection. *Seton Hall L. Rev*., 47, 809.

Schryver, K. (2019, August 1). The Future of Data Privacy in the United States. *CPO Magazine.* Available: https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-in-the-united-states/

Shi, P., Xu, H., & Chen, Y. (2013). Using contextual integrity to examine interpersonal information boundary on social network sites. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 35-38). New York: ACM.

Short, R., & Magaña, L. (2002). Political rhetoric, immigration attitudes, and contemporary prejudice: A Mexican American dilemma. *The Journal of Social Psychology*, 142(6), 701–712. https://doi.org/10.1080/00224540209603930

Smith, A. (2017). *What the Public Knows About Cybersecurity*. Pew Internet Project. Available: https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

Taylor, B. J. (2005). Factorial surveys: Using vignettes to study professional judgement. *British Journal of Social Work*, 36(7), 1187-1207.

Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Available at SSRN 2820060.

Wagner, K. (2018, April 11). This is how Facebook uses your data for ad targeting. *Recode.* Available: 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. https://doi.org/10.1016/j.ssresearch.2009.03.004

Zimmer, M. (2008). Privacy on planet Google: Using the theory of contextual integrity to clarify the privacy threats of Google's quest for the perfect search engine. *Journal of Business & Technology Law*, *3*(1), 109–126.

Zureik, E., Harling Stalker, L., Smith, E., Lyon, D., and Chan., Y.E. (2010). *Surveillance, Privacy and the Globalization of Personal Information: International Comparisons.* Montreal: McGill-Queen's University Press.

Appendix

Figure 1: Screenshot of a vignette as it appeared to respondents

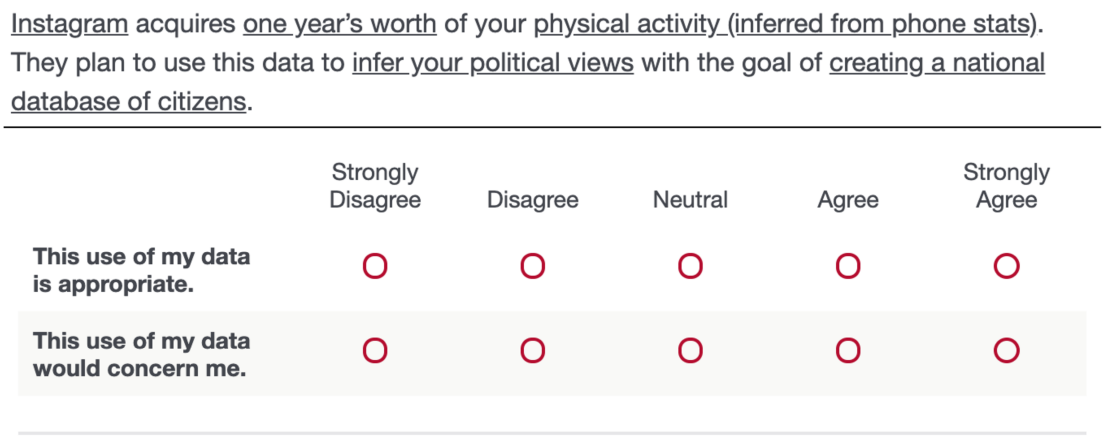


Table 1. Details of Vignette Factors

Vignette Factors	**Number of Levels**	**Factor Levels**
Actor	6	Law enforcement Your company's HR department Your doctor A social media/messaging app a respondent uses An online advertising agency Your local government
Content / Information Type	8	Text-based posts and messages Photos and video posts Web browsing search history Emails 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

Table 2. Comparing American and Dutch Mobile Privacy Concerns

	Variable		American (n=324)	Dutch (n=507)	t-value	p-value
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	0.001
		SD	(.77)	(.97)		
Mobile Concern 2	I am concerned that mobile apps are collecting too much information about me.	M	4.09	3.94	2.23	0.026
		SD	(1.00)	(.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	0.75
		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	0.001
		SD	(1.00)	(.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	0.000
		SD	(.94)	(.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	0.064
		SD	(.88)	(.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	0.000
		SD	(.91)	(.89)		
		M	4.16	4.08	1.23	0.22

Mobile Concern 8	I am concerned that mobile apps may share my personal information with other entities without getting my authorization.	SD	(.92)	(.89)

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

Table 3. Comparing American and Dutch Trust in Social Institute

	Variable		American (n=324)	Dutch (n=507)	t-value	p-value
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	0.000
		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	-3.6	0.000
		SD	(1.20)	(1.09)		
Trust in American Companies	Most of the time I trust American companies to do what is best for consumers.	M	2.27	2.29	-0.23	0.82
		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	0.000
		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	0.000
		SD	(1.21)	(1.11)		

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

Table 4. Comparing American and Dutch Resignation/Fatalism

	Variable		American (n=324)	Dutch (n=507)	t-value	p-value
Fatalism belief 1	There is nothing I can do to protect my privacy and security online.	M	2.20	2.64	-6.12	0.000
		SD	(.99)	(1.02)		
Fatalism belief 2	In the online world, privacy does not exist anymore.	M	2.86	3.15	-8.33	0.000
		SD	(.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	0.82

		SD	(.97)	(1.05)		
Fatalism belief 4	I have no control over the information I share online.	M	2.15	2.53	-5.6	0.000
		SD	(.89)	(.97)		

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

Table 5. Comparing American and Dutch Pragmatism

	Variable		American (n=324)	Dutch (n=507)	t-value	p-value
Pragmatism belief 1	I might trade my personal data for convenience.	M	2.50	2.61	-7.54	0.00
		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	-13.81	0.00
			(1.20)	(1.17)		

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

Table 6. Summary Statistics for Linear Mixed-Effects Models (DV= Data Use Concern)

		American		**Dutch**	
Fixed Effect (Between-subject)		**F**	**Sig.**	**F**	**Sig.**
	Intercept	35.50	<.001	56.16	<.001
	Individual Characteristics				
	Age	6.66	<.01	13.78	<.001
	Gender	-[a]	-	-	-
	Education	-	-	3.62	0.06
	Mobile Privacy Concern	79.13	<.001	30.71	<.01
	Trust	4.42	<.05	-	-
	Self-efficacy	-	-	-	-
	Fatalism belief	4.21	<.05	13.03	<.001
	Pragmatism belief	5.74	<.05	3.5	0.06
	Vignette Attributes				
	Actor	7.68	<.001	45.81	<.001
	Amount	21.99	<.001	-	-
	Content	15.00	<.001	1.83	0.08
	Inference	19.23	<.001	13.15	<.001

	Purpose	19.12	<.001	17.98	<.001
Random Effect (Within-subject)		**Wald Z[b]**	**Sig.**	**Wald Z[b]**	**Sig.**
	Residual	70.66	<.001	78.77	<.001
	Intercept	12.21	<.001	14.72	<.001
Model fit： Bayesian Information Criterion (BIC):		BIC[c] =23612.05		BIC[c]=28808.12	

Notes:
a. The parameters marked with "-" have p values larger than .10.
b. A Wald Z test is used to decide if the random effect is needed. In our cases, null hypotheses of no random effect are rejected, with p<.001. We do need to include a random intercept.

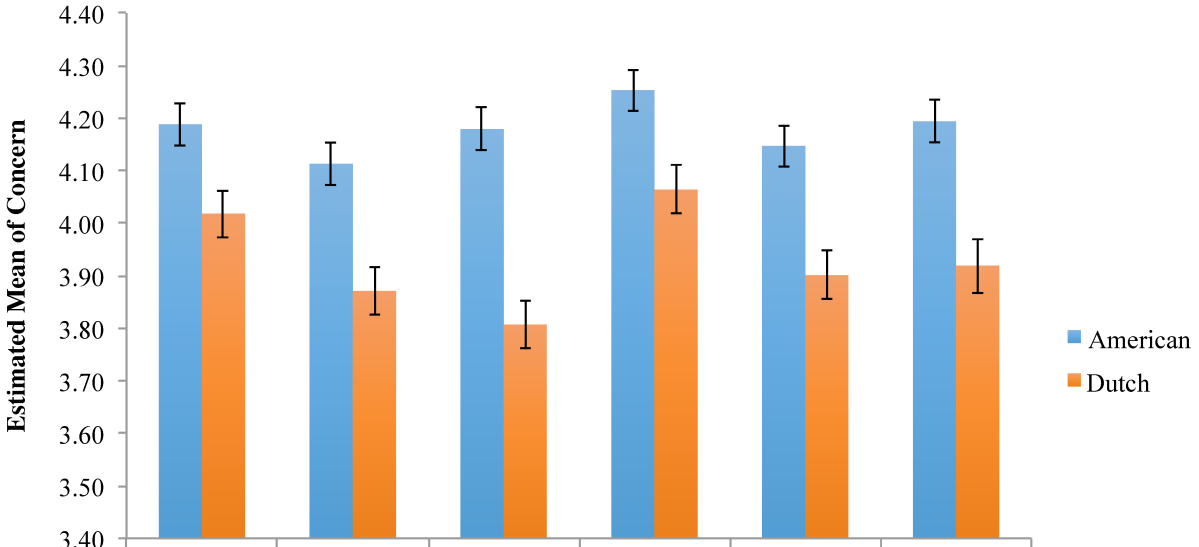
Table 7. Model Details: Estimated Effects of Individual Characteristics (DV= Data Use Concern)

	American	**Dutch**
	Estimate Coefficient (standardized)	
Age	.01*	.01*
Gender (=male)	-.00	-.07
Education	.02	.11
Mobile Privacy Concern	.54***	.37***
Trust	-.09*	-.00
Self-efficacy	0	0
Fatalism belief	-.11*	-.25***
Pragmatism belief	-.09*	.08

Table 8. Model Details: Estimated Effects of Vignette Factors (DV= Data Use Concern)

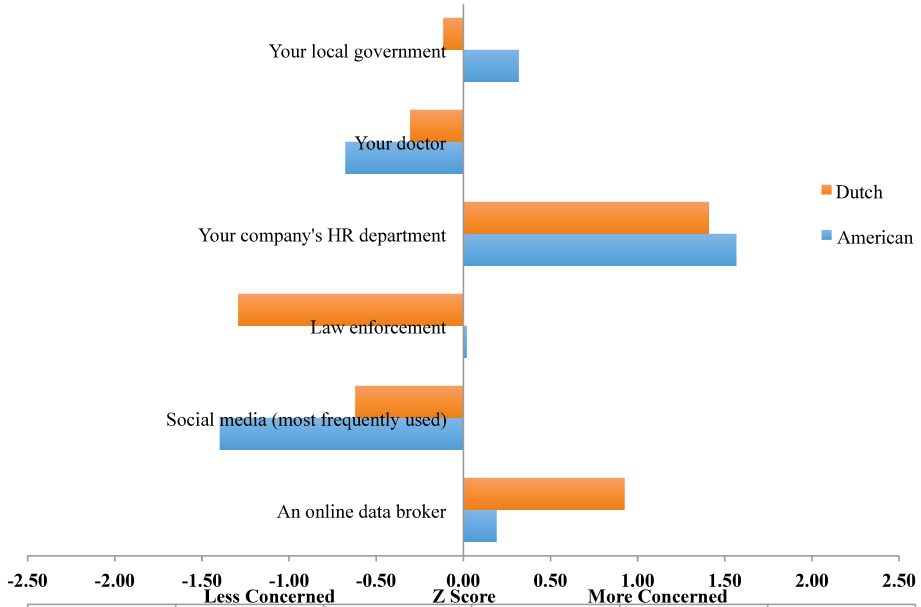
	American	**Dutch**
Coefficient (standardized)		Estimate
Actors		
An online data broker	-0.01	.10**
Social media (most frequently used)	-.09**	-0.05
Law enforcement	-0.02	-.11***
Your company's HR department	.06*	.15**
Your doctor	-0.05	-0.02
Your local government	_ [a]	_ [a]
Content		
Emails	.08**	0.03
Phone call log data	0.01	0.03
Phone's location data	-0.05	0.02
Photos and video posts	-0.01	0.08
Physical activity (inferred from phone stats)	-.16***	0.02
Social media posts	-.12***	-0.03
Text-based posts and messages	0	0.04
Web browsing search history	_ [a]	_ [a]
Amount		
One week’s worth	-.11***	-0.01
One year’s worth	-0.02	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	0.05	-.14***
Improving traffic flow in your region	-.29**	-.18***
Increasing productivity	0.03	0.03
Preventing or reducing criminal activity	.09***	-.06**
Providing you with personalized advertising	.09**	0.05
Reduce binge drinking	0.02	.05*
Reducing the spread of disease	_ [a]	_ [a]

Figure 2. (Non-Normalized) Estimated Mean of Concern by Actor



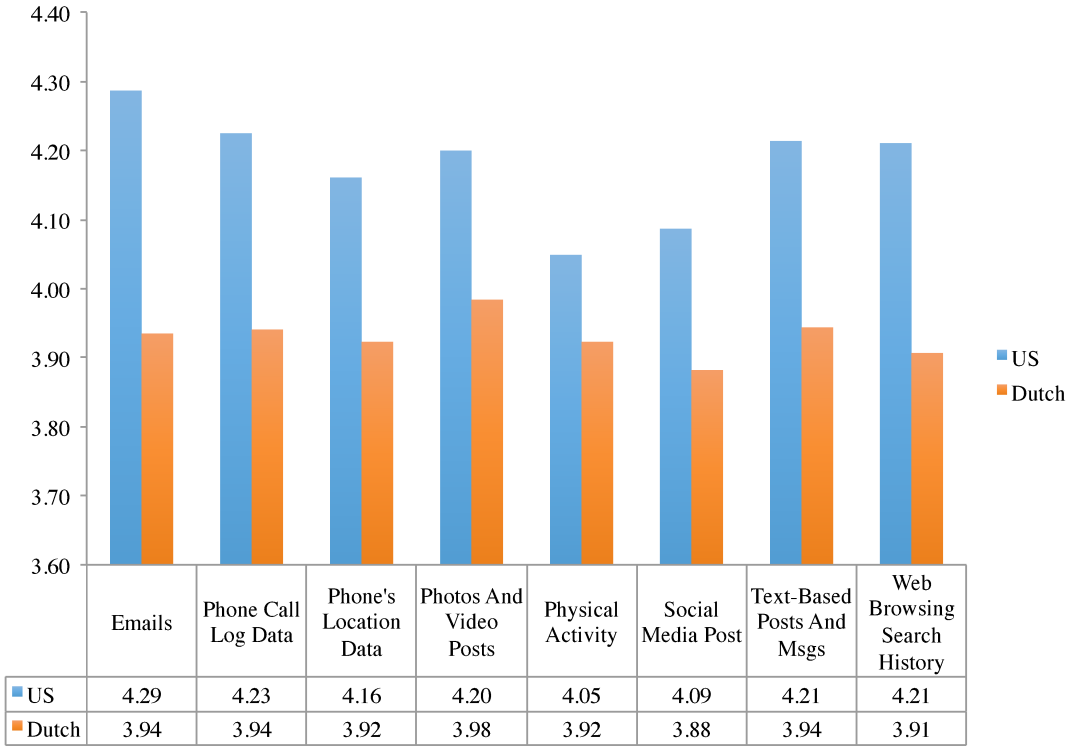
	Online data broker	Social media	Law enforcement	Company's HR department	Doctor	Local government
American	4.19	4.11	4.18	4.25	4.15	4.19
Dutch	4.02	3.87	3.81	4.06	3.90	3.92

Figure 3. Normalized Z Scores of Data Concerns by Actor



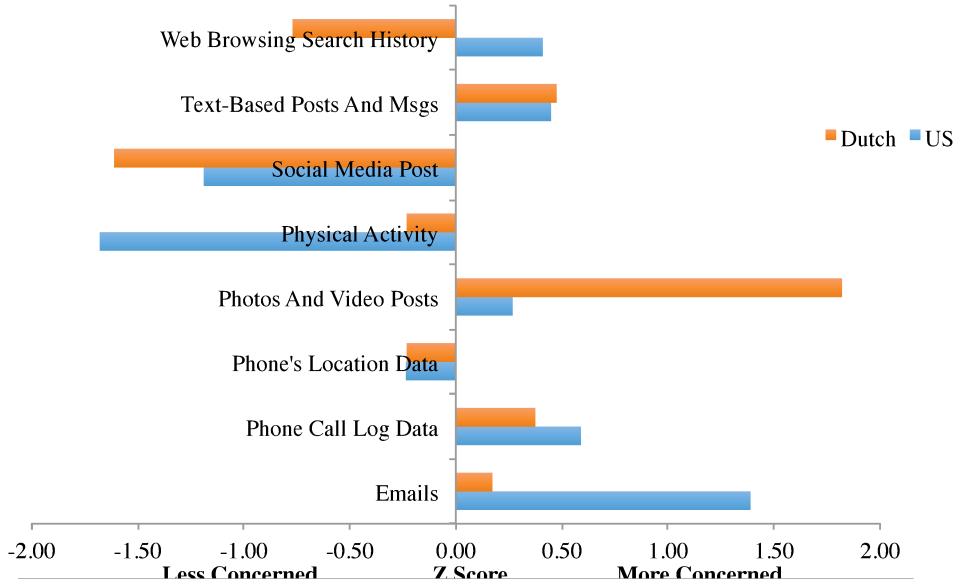
	An online data broker	Social media (most frequently used)	Law enforcement	Your company's HR department	Your doctor	Your local government
Dutch	0.92	-0.62	-1.29	1.41	-0.30	-0.12
American	0.19	-1.40	0.02	1.57	-0.68	0.32

Figure 4. (Non-Normalized) Estimated Mean of Concern by Content



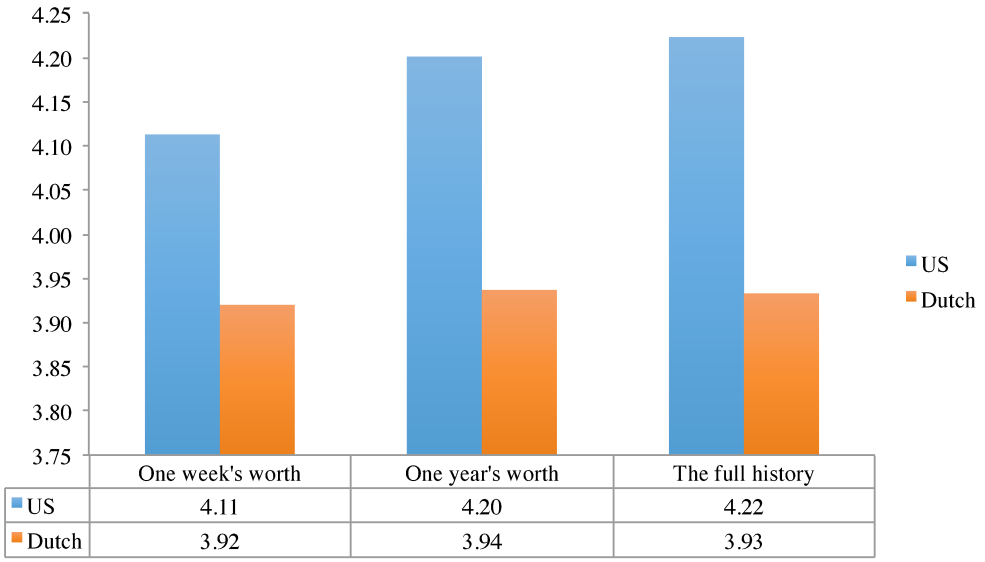
	Emails	Phone Call Log Data	Phone's Location Data	Photos And Video Posts	Physical Activity	Social Media Post	Text-Based Posts And Msgs	Web Browsing Search History
US	4.29	4.23	4.16	4.20	4.05	4.09	4.21	4.21
Dutch	3.94	3.94	3.92	3.98	3.92	3.88	3.94	3.91

Figure 5. Normalized Z Scores of Data Concerns by Content



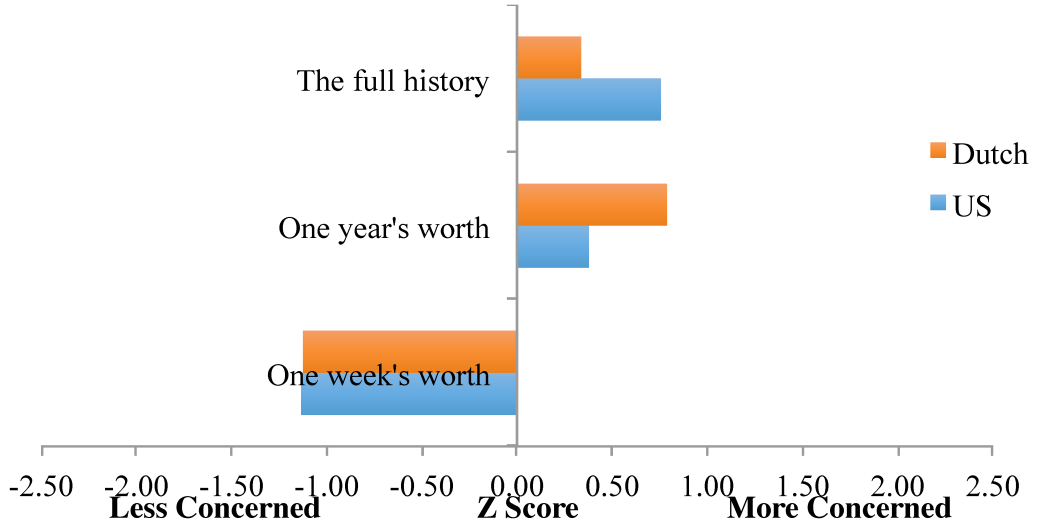
	Emails	Phone Call Log Data	Phone's Location Data	Photos And Video Posts	Physical Activity	Social Media Post	Text-Based Posts And Msgs	Web Browsing Search History
Dutch	0.17	0.37	-0.23	1.82	-0.23	-1.61	0.48	-0.77
US	1.39	0.59	-0.24	0.27	-1.68	-1.19	0.45	0.41

Figure 6. (Non-Normalized) Estimated Mean of Concern by Data Amount



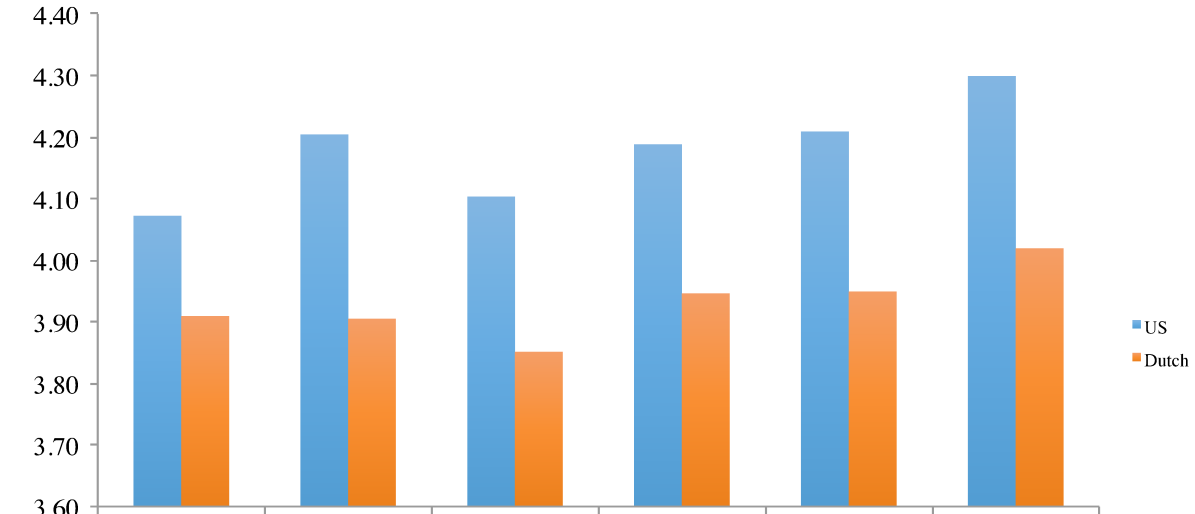
	One week's worth	One year's worth	The full history
US	4.11	4.20	4.22
Dutch	3.92	3.94	3.93

Figure 7. Normalized Z Scores of Data Concerns by Data Amount



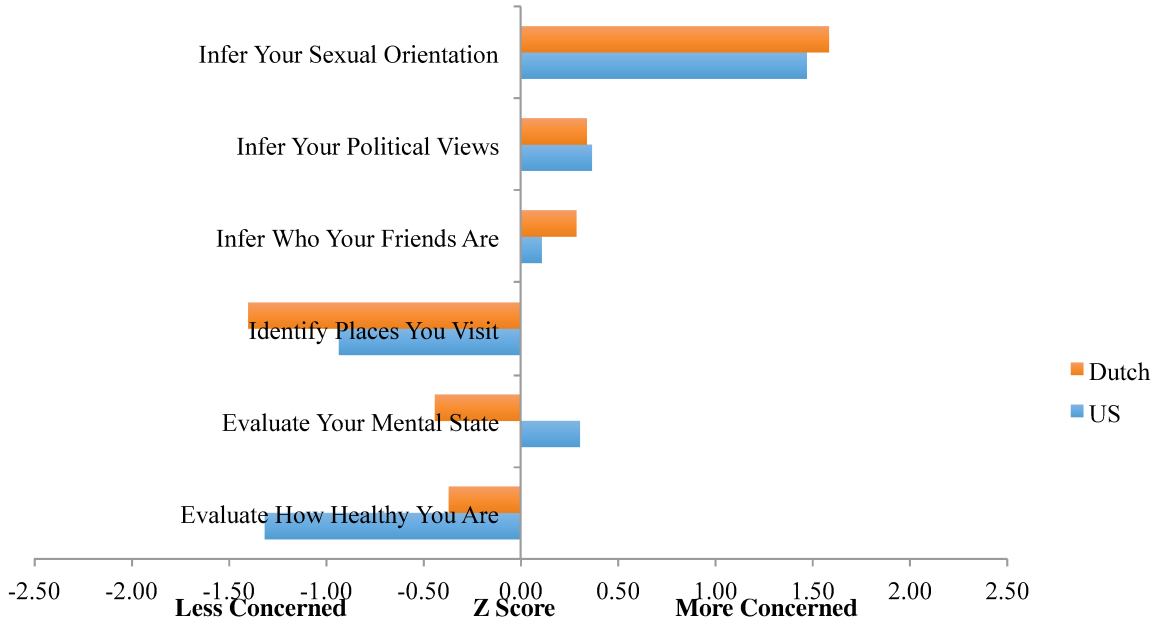
	One week's worth	One year's worth	The full history
Dutch	-1.13	0.79	0.34
US	-1.13	0.38	0.76

Figure 8. (Non-Normalized) Estimated Mean of Concern by Inference



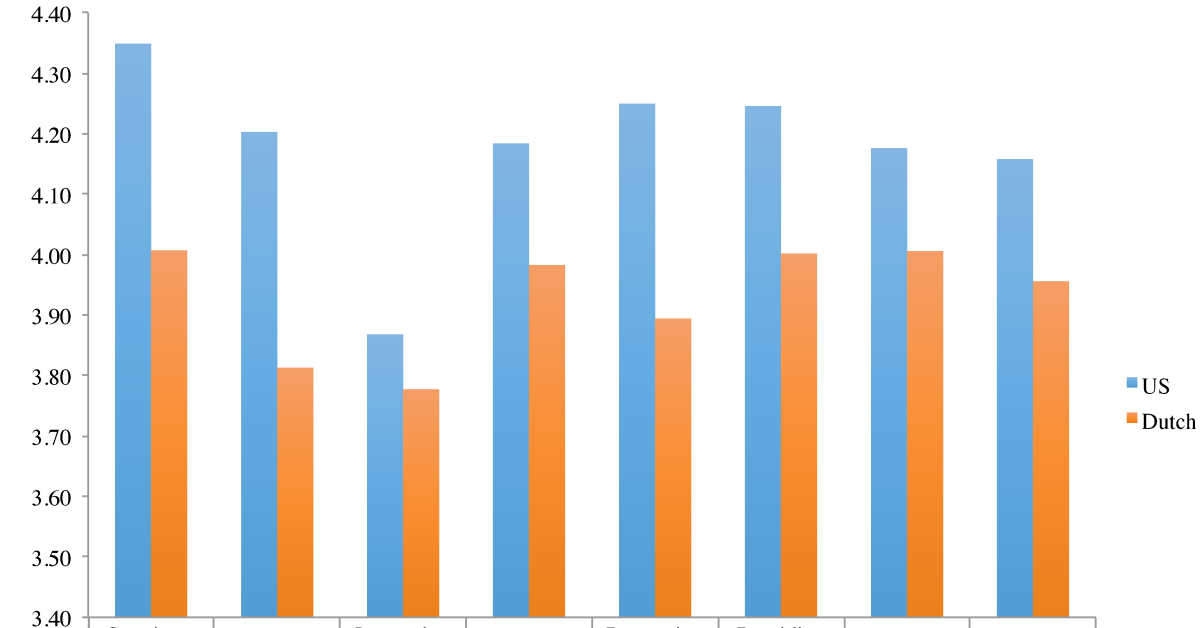
	Evaluate How Healthy You Are	Evaluate Your Mental State	Identify Places You Visit	Infer Who Your Friends Are	Infer Your Political Views	Infer Your Sexual Orientation
US	4.07	4.20	4.10	4.19	4.21	4.30
Dutch	3.91	3.91	3.85	3.95	3.95	4.02

Figure 9. Normalized Z Scores of Data Concerns by Inference



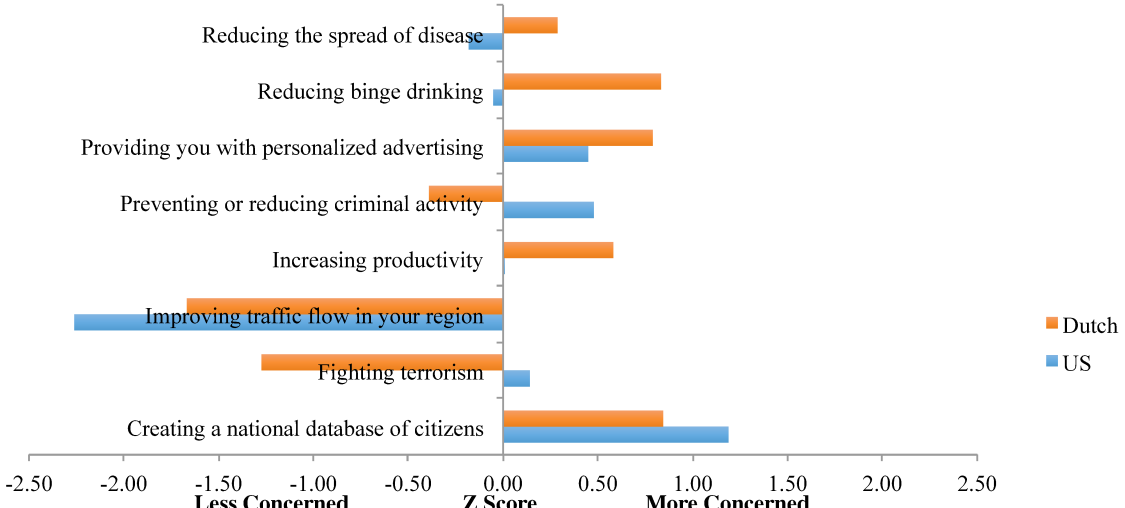
	Evaluate How Healthy You Are	Evaluate Your Mental State	Identify Places You Visit	Infer Who Your Friends Are	Infer Your Political Views	Infer Your Sexual Orientation
Dutch	-0.37	-0.44	-1.40	0.29	0.34	1.58
US	-1.31	0.30	-0.93	0.11	0.37	1.47

Figure 10. (Non-Normalized) Estimated Mean of Concern by Purposes



	Creating a national database of citizens	Fighting terrorism	Improving traffic flow in your region	Increasing productivity	Preventing or reducing criminal activity	Providing you with personalized advertising	Reducing binge drinking	Reducing the spread of disease
US	4.35	4.20	3.87	4.18	4.25	4.25	4.18	4.16
Dutch	4.01	3.81	3.78	3.98	3.89	4.00	4.01	3.96

Figure 11. Normalized Z Scores of Data Concerns by Purpose



	Creating a national database of citizens	Fighting terrorism	Improving traffic flow in your region	Increasing productivity	Preventing or reducing criminal activity	Providing you with personalized advertising	Reducing binge drinking	Reducing the spread of disease
Dutch	0.84	-1.27	-1.67	0.58	-0.39	0.79	0.832185717	0.286490165
US	1.19	0.14	-2.26	0.00	0.48	0.45	-0.052572605	-0.181614455