DIFFERENCES IN ONLINE PRIVACY AND SECURITY ATTITUDES BASED ON ECONOMIC LIVING STANDARDS: A GLOBAL STUDY OF 24 COUNTRIES

Research paper

Rho, Eugenia, Ha Rim, University of California, Irvine, hrrho@uci.edu

Kobsa, Alfred, University of California, Irvine, kobsa@uci.edu

Nguyen, Carolyn, Microsoft Corporation, cnguyen@microsoft.com

Abstract

This work explores online privacy and security attitudes from 24,143 individuals across 24 countries with diverse economic living standards. By using k-mode analysis, we identified three distinct profiles based on similarity in Internet security and privacy attitudes measured by 83 items. By comparing the aggregated dissimilarity measures between each respondent and the centroid values of the three profiles at the country level, we assigned each country to their best-fitting privacy profile. We found significant differences in GDP per capita between profiles 1 (highest GDP) to 3 (lowest). People in profiles with higher GDP per capita have significantly greater privacy concerns in relation to information being monitored or bought and sold. These individuals are also more reluctant towards government surveillance of online communication as well as less likely to agree that governments should work with other public and private entities to develop online security laws. As economic living standards improve, the proportion of individuals increases in profile 1, decreases in profile 2, and most rapidly drops in profile 3. To the best of our knowledge, it is the first research that systematically examines country-level privacy in relation to a national economic variable using GDP per capita.

Keywords: Privacy, security, GDP per capita, economic living standards, clustering.

1 Introduction

Rise in Internet access and mobile networks across the world have allowed online technologies to increasingly permeate commerce, social interactions, and numerous aspects of people's daily lives. However, it is well known that technological adoption and experience can vary by people's income or national economic living standards (Kiiski and Pohjola, 2002; Parente and Prescott, 1994). For example, consumers from wealthier nations are often early adopters of new technologies created by companies that are primarily based in western headquarters (Kar, 2016; McCaskill, 2015). Compared to developed economies, public discourse around information privacy laws is more recent in developing nations (Nwanne, 2014; Nyst, 2012). Such differences in country-level characteristics related to economic living standards may influence affordances around technology adoption, regulation, as well as perspectives around the risks and benefits associated with online technologies. The aim of this research was to study the differences in online privacy and security attitudes on a world-wide scale, and to examine how these attitudes differ based on country-level characteristics. Through this study, we tried to 1) see whether people across a global population can be grouped into distinct profiles based on similarity in online privacy and security preferences, 2) determine which countries best fit into each profile, and 3) understand how these privacy profiles are similar and different from one another. The paper is organized as follows: we introduce related literature on cross-country privacy in section 2, provide an overview of our research methods in section 3, and present our analysis in section 4. In section 5, we showcase our findings and discuss implications in section 6.

2 Related Work

2.1 Country-level privacy research tends to have a cultural focus

Several global privacy studies in Information Systems (IS) research link privacy and security concerns with country-level characteristics, such as country of residence (Anton et al., 2010), native language (Steenkamp and Geyskens, 2006), institutional trust (Dinev and Hart, 2006), and regulatory environments (Bellman et al., 2004; Milberg et al., 1995). However, most of these studies examine cross-national privacy from a cultural rather than economic perspective. In fact, in the few cases where privacy concern is examined at a macro-level across a global set of countries, scholars have relied on cultural factors using Hofstede's dimensions, which were developed to measure cultural differences among countries using factor analysis on data collected from a worldwide survey between 1967 and 1973 (Hofstede, 1980). Over the years, researchers have validated and further updated the model to include the following six cultural dimensions: power distance, individualism, masculinity, pragmatism, uncertainty avoidance, and indulgence (Hofstede, 2011, 2001).

Many IS scholars have compared privacy attitudes across nations of different cultures in relation to these dimensions (Cho and Lee, 2008; Ciganek and Francia, 2009; Li et al., 2017; Marshall et al., 2008; Park and Jun, 2003; Steenkamp and Geyskens, 2006; Zhao and Jiang, 2011). Most recently, Bauer and Schiffinger (2016) investigated how cultural dimensions moderate people's risk and benefit assessment of online self-disclosure in 13 countries, showing that uncertainty avoidance, power distance, and long-term orientation affect privacy concerns in revealing one's information online. Cultural dimensions are also significant predictors of information privacy concern related to the intention and actual use of instant messaging for both Chinese and American users (Lowry et al., 2011), as well as differences in Facebook privacy concerns between Moroccan and American individuals (Veltri et al., 2011).

While Hofstede's dimensions are one of the most widely accepted and used country-level constructs associated with culture, there are some cases where scholars have attributed different scores along these dimensions for the same country (Bradley, 1999; Naumov and Puffer, 2000). Furthermore, Milberg et

al. (1995) showed that a country's individualism, power distance, and masculinity scores were positively, but uncertainty avoidance negatively, associated with information privacy concerns. However, Bellman et al. (2004) demonstrated opposite findings: greater individualism, power distance, and masculinity predicted lower privacy concerns while uncertainty had no significant effect. As such, cultural factors are extremely diverse, subjective and therefore, can have limitations when quantified into a measurement construct (Hofstede, 2006; Naumov and Puffer, 2000) as the only lens to examine differences in privacy attitudes across many countries.

Our work eschews such limitations by introducing a national economic variable to compare privacy and security attitudes across a global set of countries. Instead of associating a country to its cultural attributes, we use its Gross Domestic Product (GDP) per capita to examine country-level privacy across different levels of economic development and living standards.

2.2 Lack of diverse global privacy surveys in academic research

A great methodological challenge in cross-country privacy research is involving a truly global and diverse set of participants especially from non-western and developing nations (Borena and Ejigu, 2013). Most well-known privacy constructs have been developed by surveying residents in western or developed countries (Buchanan et al., 2007; Dinev and Hart, 2004; Malhotra et al., 2004; Smith et al., 1996; Stewart and Segars, 2002). These surveys are often contextualized to the social and technological norms and lifestyles based on the participant country's average living standards that are well above most emerging economies. Thus, there is a lack of locally well-tested and validated instruments for non-western and developing nations. This in return, makes it highly difficult to conduct surveys that are appropriately contextualized to capture privacy concerns in such countries. This challenge is indeed reflected in the significant limitation in IS literature where scholars have pointed out the dearth of privacy work on countries that are non-western or considered developing economies (Anteneh et al., 2015). Furthermore, most IS work on cross-national privacy and security attitudes typically involve two countries (Krasnova and Veltri, 2011; Zhao and Jiang, 2011). Focusing on two nations can offer in-depth comparisons of privacy attitudes, but not a comparative view in relation to a more diverse set of countries from different regions of the world (Bauer and Schiffinger, 2016).

A major novelty of this work is the implementation of the broadest world-wide survey on online privacy and security concerns administered to approximately 24,000 individuals across 24 countries from a diverse economic development spectrum. Out of the 24 countries, twelve are considered developing nations according to the International Monetary Fund's 2015 World Economic Outlook Report[1]. Prior to this survey, the European Commission reported findings on attitudes towards identity management, data protection, and privacy across 27 countries based on a 2010 survey on approximately 27,000 individuals (EC, 2011). However, the survey was only administered to the citizens from the member states of the European Union, leaving out countries from other regions of the world with lower living standards. Currently, the CIGI survey used in this study is the largest global privacy survey that has drawn participants from both western and non-western countries with varying degrees of national economic wealth.

2.3 Privacy, technology, and economic living standards

Historically, countries with varying levels of economic wealth have adopted technologies at different paces and manners, which in return shaped relationships, expectations, and social norms around technology accordingly (Winner, 1980). The evolvement of such norms can affect people's perception of privacy and security towards the technology they use and are exposed to on a daily basis (Westin, 2001). For example, privacy is commonly associated with surveillance and human rights in developing nations (Nyst, 2012), but more from a commercial value perspective in most industrial countries (Rainie and Duggan, 2016). This is understandable given the different roles technology may play in people's lives based on diverse economic living standards.

[1] Poland, Turkey, Indonesia, Mexico, South Africa, Brazil, India, Egypt, Pakistan, Nigeria, Kenya, and Tunisia

For example, in India, where the government has been trying to push for a biometric ID card program to address some of the nation's worst poverty issues, nearly 1.2 billion citizens or 92% of India's population have registered for the Aadhaar scheme that "links fingerprints and iris scans to a unique 12-digit number" (Iyengar, 2017). Despite severe criticisms of government surveillance, the program is considered one of the country's most wide-scale efforts to increase accountability in providing millions of the nation's poorest with access to basic health, education, and welfare assistance – problems that still exist, but are much less endemic and smaller in scale among wealthier nations. When sacrificing privacy implies getting access to basic means of life as opposed to a car sharing company knowing one's location, people may weigh risk perceptions around personal information differently. The value gained by sacrificing privacy in the modern digital economy can have different implications based on one's living standards.

To the best of our knowledge, extant literature has not explored the relationship between privacy concern and economic living standards, especially at a global scale. However, we believe the subject is an important aspect to consider. So far, the topically closest finding stems from Acquisti et al. (2006)'s work where the authors show that privacy concern is positively correlated with income based on a 2004 survey administered to 119 people. However, 83% of the survey respondents were US citizens and all participants were studying or have studied at a higher education institution. Hence, the sample was heavily skewed towards the highly educated and not culturally diverse in terms of nationality. Through this work, we incorporate GDP per capita measures across 24 countries, and thereby introduce a comparative examination of privacy concern in relation to economic living standards from a global sample.

3 Research Method

3.1 Data collection

The data for this study was collected by the Centre for International Governance Innovation (CIGI) and Ipsos, a global marketing research company as part of the 2016 Global Survey on Internet Security and Trust (CIGI-Ipsos). The survey was administered across 24 countries to 24,143 internet users between November 20, 2015 and December 4, 2015. The countries included in this survey are: Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey and the United States. The survey was administered to approximately 1000+ individuals in each country.

Twenty of the countries utilized the Ipsos Internet panel system while Tunisia was conducted via computer-assisted telephone interviewing (CATI), a telephone surveying technique in which the interviewer follows a script provided by a software application (Groves and Mathiowetz, 1984; Lavrakas, 1987). For survey participants in Kenya, Nigeria and Pakistan, face-to-face interviewing was used given the online constraints in these countries as well as the length of the survey. All respondents were recruited via random probability sampling ("Survey Methods, Ipsos MORI"). The precision of survey responses based on the Ipsos Internet panel system is calculated using a credibility interval (Gelman, 2004). In this case, a poll of 1,000 is accurate to +/- 3.5 percentage points. For those surveys conducted by CATI and face-to-face, the margin of error is +/-3.1, 19 times out of 20. Respondents from the U.S. and Canada were between the ages of 18-64, and 16-64 for all other countries.

The survey includes 97 questions encompassing issues related to online privacy, security, and attitudes towards government and corporate roles in the protection of personal data. All responses are based on a 5-point Likert scale (Likert, 1932). For the study, three independent researchers coded each question for its relevance to online privacy and security issues and determined that 14 questions were not relevant based on past IS privacy surveys widely used and validated by scholars (Altman, 1975; Bellman et al., 2004; Malhotra et al., 2004). The inter-rater reliability among the three coders was high with Pearson's $r(33) = .95$, $p<.001$. These 14 questions were excluded and only the remaining 83 items subjected to the analyses described below. Furthermore, we excluded 276 respondents due to missing data.

3.2 Clustering of online privacy, security, and trust attitudes

In order to identify the emergent groups based on similarity in online privacy and security attitudes, we used the k-mode algorithm (Huang, 1998, 1997). K-mode is a variation of the k-means algorithm that allows clustering of large categorical data sets. We chose k-mode over k-means for this very reason, given that the survey responses included many categorical values. Unlike k-means that only allows clustering of continuous responses, k-mode replaces cluster means with modes and uses a simple matching dissimilarity function (Kaufman and Rousseeuw, 1990) to compute the distance between categorical objects (Huang, 1998). In other words, the algorithm updates the modes with the most frequently occurring categorical attributes in the clustering process and divides the categorical objects into an optimal number of groups such that the distance from objects to the assigned cluster modes is minimized (Huang, 1998; Lee and Kobsa, 2017).

Using the kmode function in the R 'klaR' package (Neumann), we clustered participants solely based on their responses to the 83 questions coded as relevant to online privacy and security attitudes. We excluded demographic variables such as age, income, and gender, because we wanted to create privacy profiles solely based on online security and privacy preferences to which we could map the countries into these profiles regardless of other variables that are known to affect privacy.

4 Analyses

4.1 Three distinct privacy profiles across a global population

In order to determine the optimal number of clusters we used the Elbow method (Kodinariya, 2013) by calculating the sum of errors in each clustering procedure as we varied the number of clusters (k) from 2 to 7 with a limit of 100 iterations. The sum of error is the sum of the distances between each individual's categorical response vector (or each person's response to the 83 questions as one vector) and the cluster's centroid or mode. The sum of error for cluster k (SE_k) can be expressed as follows (Lee and Kobsa, 2017):

$$SE_k = \sum_{i=1}^{k} \sum_{x \epsilon c_i} d(x, c_i)$$

Here, k is the number of cluster while x is each individual response vector belonging to the i^{th} cluster and c_i is the mode for that i^{th} cluster. By calculating the difference between SE_k and SE_{k-1}, we found that the optimal number of clusters was 3. In other words, the largest decrease in the sum of errors occurred when we increased the number of clusters from 2 to 3 as shown in Table 1.

Number of clusters (k)	Sum of Errors (SE_k)	Error Difference (SE_{k-1})
2	389,909	
3	**253,724**	**-136,184**
4	184,036	-69,688
5	145,056	-38,981
6	117,919	-27,137
7	86,427	-31,492

Table 1. Clustering sum of errors (for k= 2 to 7) show that the largest decrease in error difference occurs when the optimal number of cluster is 3.

Hence, from our analysis we were able to identify three distinct groups of respondents in our global data set based on their similarity in online privacy and security attitudes. In the following, we will call them profiles 1, 2, and 3.

4.2 Assignment of countries to profiles based on dissimilarity measure

After identifying the three profiles across our global data set, we used the simple matching dissimilarity measure (Kaufman and Rousseeuw, 1990) to assign each country to the best-fitting profile. For each country, we calculated three sums of errors based on the distance or the dissimilarity measure between all the categorical response vectors of the individuals in that country to each of the three profiles' centroid values. Each country was then assigned to the profile with the lowest sum of error.

More specifically, let X and C be two categorical objects described by m categorical attributes. In our case, X would be the vector of responses for an individual and C, the vector of centroid values for a profile, both with m categorical attributes (83 questions). The dissimilarity measure between X and C can be defined by the total mismatches of the corresponding attribute categories of the two objects, which can be expressed as follows (Huang, 1998):

$$d(X, C) = \sum_{j=1}^{m} \delta(x_j, c_j)$$

where

$$\delta(x_j, c_j) = \begin{cases} 0 & (x_j = c_j) \\ 1 & (x_j \neq c_j) \end{cases}$$

The smaller the number of mismatches, the more similar the two objects, or in other words, the more fitting the respondent to that profile. Following this logic, we calculated three sum of errors (SE_c) for each country based on the aggregated dissimilarity measures between all the individuals in that country and the centroid for each of the three profiles. Then we compared the three sum of error values and assigned the country to the profile whose sum of error was smallest. The sum of error between all the respondents of a country and the centroid for profile 1 can be expressed as the following equation:

$$SE_1 = \sum_{i=1}^{r} \sum_{j=1}^{m} \delta(x_j, c_j)$$

Here, r is the total number of respondents in a country, m is the number of categorical attributes (83 questions), x is the response value of a respondent, and c is the response value of the profile centroid, as described earlier.

Using this method, we assigned each country to their respective profiles as summarized in Table 2. As shown in the table, the sum of error for Great Britain is smallest for profile 1 (SE_1=30,785) and largest for profile 3 (SE_3=45,092), suggesting that individuals in Great Britain responded most similarly to those in profile 1 and least so to those in profile 3. Likewise, respondents in Indonesia are most similar in terms of privacy and security preferences to those in profile 2 than those in profile 1, and least similar to those in profile 3 ($SE_2 < SE_1 < SE_3$). Finally, Kenya's respondents have most similar privacy and security preferences to individuals classified as profile 3 (SE_3=34,768) and least similar to those classified as profile 1(SE_3=48,153).

After assigning each country based on the sum of dissimilarity measures from the centroid, we also looked at the distribution of profiles across each country. For example, as shown in Table 2, 78% of the respondents from Germany belong in profile 1, 13% in profile 2, and 8% in profile 3. The mean distribution for each profile across all countries are indicated on the bottom of this table as $\mu_1 = 49\%$ for profile 1, $\mu_2 = 25\%$ for profile 2, and $\mu_3 = 26\%$ for profile 3.

		Dissimilarity measures between profile centroids and all respondents from each country			Percentage of respondents in each profile by country			2015 GDP per capita	
Profile	Country	SE_1	SE_2	SE_3	P_1	P_2	P_3	($K)	Mean
1	Japan	**30522**	38776	46815	84%	10%	6%	37.3	38.9
	Great Britain	**30785**	37188	45092	75%	15%	10%	41.3	
	Germany	**31587**	38120	45975	78%	13%	8%	47.3	
	France	**31592**	37518	45193	74%	17%	9%	39.7	
	Canada	**32202**	38503	45335	74%	15%	11%	44.3	
	Hong Kong	**32375**	37394	46835	71%	21%	8%	56.7	
	South Korea	**32629**	37085	45937	69%	22%	9%	34.5	
	Australia	**32826**	37940	45489	69%	19%	12%	45.5	
	Poland	**32943**	37355	43368	63%	21%	15%	26.1	
	Italy	**33027**	36154	45129	60%	29%	11%	35.9	
	Sweden	**33830**	39729	47459	73%	17%	10%	46.4	
	China	**35859**	37879	45305	52%	33%	15%	14.2	
	U.S.	**36533**	40987	47723	61%	23%	16%	55.8	
	Turkey	**37407**	38986	40247	41%	25%	34%	19.6	
2	Indonesia	36372	**35706**	41099	36%	40%	25%	11.0	12.3
	Mexico	40096	**37617**	40554	26%	42%	33%	17.3	
	South Africa	38338	**37740**	39898	34%	33%	33%	13.2	
	Brazil	38802	**38265**	38644	30%	31%	39%	15.4	
	India	39976	**39015**	41369	31%	39%	31%	6.1	
	Egypt	40778	**39570**	40102	29%	32%	39%	10.9	
3	Pakistan	35552	33958	**30994**	20%	25%	55%	5.0	6.4
	Nigeria	46445	40895	**33766**	5%	25%	69%	6.0	
	Kenya	48153	39880	**34768**	2%	32%	65%	3.1	
	Tunisia	44003	43369	**36225**	18%	14%	68%	11.4	
					μ_1=49%	*μ_2=25%*	*μ_3=26%*		

Table 2. Profile assignment of countries based on dissimilarity measures, distribution of respondents in each profile, and GDP per capita for each country (in 1,000 US$).

5 Findings

5.1 Difference in GDP per capita across profiles

As shown in Table 2, for countries in profiles 1, 2 and 3, the average GDP per capita is $38.9K, $12.3K and $6.4K, respectively. A one-way ANOVA indicates significant differences in the mean GDP per capita among the three profiles, $F(2, 22797) = 3231.8$, $p < .001$, $\eta_p^2 = .22$. The effect size of .22 was also very large (Miles and Shevlin, 2001; Rice and Harris, 2005), suggesting that approximately 22% of variance in the profiles were attributable to GDP per capita. Post hoc pairwise comparisons of the mean GDP per capita using Tukey's Honestly Significant Difference procedure also showed significant pair-wise differences in GDP per capita between profile 1 and profile 2 and between profile 2 and profile 3 ($p < .001$).

5.2 Profile membership and GDP per capita

The results of a Pearson correlation test also indicated a strong positive association between GDP per capita and the percentage of respondents in profile 1, ($r(22) = .88$, $p < .001$). In contrast, GDP per capita was negatively related to the percentage of respondents in profile 2 ($r(22) = -.63$, $p < .001$) and profile 3 ($r(22) = -.80$, $p < .001$).

To further examine the relationship between a country's macroeconomic performance and the distribution of respondents in the three profiles, we used linear regression to test if a country's GDP per capita significantly predicted the distribution of respondents in each of the three profiles. We ran three linear regression models to predict the percentage of respondents in profile 1, 2, and 3 based on GDP per capita for each country using the following equation

$$Y_c = \beta_0 + \beta_1 x$$

where Y is the percentage of individuals in profile c, β_0 is the intercept coefficient, and β_1 is the 2015 GDP per capita in US dollars.

Based on the regression results, a significant regression equation was found for all three models:

$$\text{Model 1: } Y_1 = 1.526 \times 10^{-1} + 1.255 \times 10^{-5} x$$

$$\text{Model 2: } Y_2 = 3.355 \times 10^{-1} - 3.292 \times 10^{-6} x$$

$$\text{Model 3: } Y_3 = 5.123 \times 10^{-1} - 9.291 \times 10^{-6} x$$

Based on Model 1, for every $10,000 increase in GDP per capita in a given country, there is a 12.6% increase in the percentage of people in profile 1 ($R^2 = .77$, $F(1, 22) = 77.81$, $p < .001$). By contrast, every $10,000 increase in per capita income predicts a 3.3% decrease in the percentage of people in profile 2 ($R^2 = .39$, $F(1, 22) = 15.57$, $p < .001$) according to Model 2 and a 9.3% decrease in profile 3 ($R^2 = .61$, $F(1, 22) = 37.65$, $p < .001$) based on Model 3. The linear regression lines are visualized in Figure 1. As a country's economic performance increases, the distribution of people in profile 1 rises while the proportion of those in profile 2 and 3 decreases. Interestingly, the rate of decrease in profile 3 is much sharper than in profile 2.

As shown in Figure 2, the 14 countries assigned to profile 1 have a much higher percentage of individuals clustered as profile 1 based on their online privacy and security attitudes (mean = 67.4%; median = 70.2%). Indonesia, South Africa, India, Egypt, Brazil, and Mexico (profile 2) have an average of 30.8% in profile 1 (median =30.2%) while profile 3 countries – Pakistan, Nigeria, Tunisia, and Kenya – have the lowest average of 11.2% (median =11.5%) of individuals in profile 1.

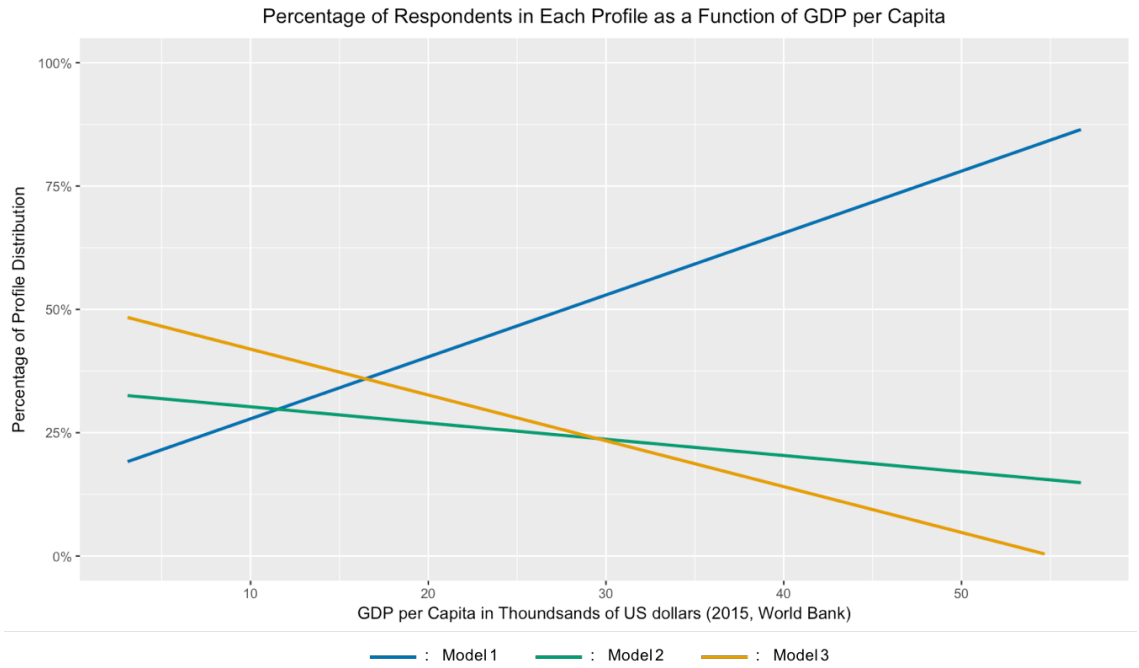

Figure 1. *As economies improve, the percentage of people in profile 1 rises while those in profile 2 and 3 decreases.*

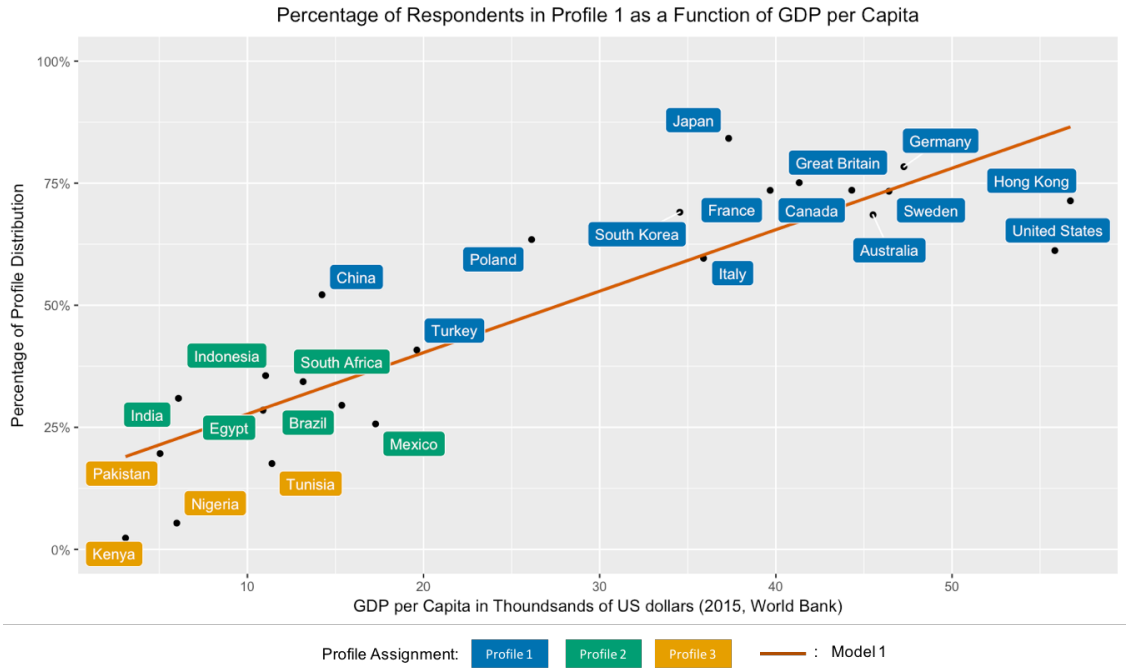

Figure 2. *The percentage of respondents belonging to profile 1 is significantly higher in countries with higher GDP per capita (2015).*

5.3 GDP per capita and concern about personal information being monitored, bought, and sold

In order to examine how the three profiles were different in terms of privacy and security attitudes, we used the survey responses to conduct a series of one-way ANOVAs and post-hoc tests[2]. In the following sections, we focus on key questions most topically relevant and frequently discussed in the IS privacy literature[3]. Our results show that online privacy concern was highest in profile 1 and lowest in profile 3, and that pairwise differences between the three profiles were statistically significant in all cases. In other words, people in profiles with a higher mean GDP per capita had significantly greater privacy concerns in several areas than those in profiles with lower economic living standards.

When asked about their "information being monitored" (Q20-2) under the increasing mobile connectivity of devices, such as phones, cars, and other things one might not be aware of, there were significant differences in the level of privacy concern among the three profiles, $F(2, 22797) = 3231.8$, $p < .001$, $\eta p^2 = .06$. Concern level was highest among those in profile 1, then in 2 and 3. Post-hoc comparisons using the Tukey HSD test ($p < .001$) showed that the differences were statistically significant. Although the effect size was smaller, there were similar results regarding whether "information being bought and sold" (Q20-3) caused privacy concern among individuals, $F(2, 22797) = 3231.8$, $p < .001$, $\eta p^2 = .04$. Privacy concern was highest in the richest and lowest in the poorest profile, and the pairwise differences were statistically significant ($p < .001$). Furthermore, there were significant differences in the level of concern related to "a lack of privacy as a result of having so much information about me available on the internet" (Q20-4) among the three profiles, $F(2, 22797) = 3231.8$, $p < .001$, $\eta p^2 = .052$. Concern level was highest in profile 1 and lowest in profile 3, and the differences were statistically significant ($p < .001$).

5.4 GDP per capita and concern about government surveillance of online communication

There were significant differences in acceptance levels among the three profiles in regards to the statement that "governments should be able to find out who their suspects communicated with online" (Q10-2) when someone is suspected of a crime, $F(2, 23864) = 932.39$, $p < .001$, $\eta_p^2 = .073$. Those in profile 3 were most accepting while people in profile 1 agreed the least. The large eta-square value of .073 (Miles and Shevlin, 2001; Rice and Harris, 2005) also indicates that approximately 7.3% of the variance in acceptance levels among the three profiles are attributable to profile membership. Moreover, those in profiles with lower GDP per capita were significantly more likely to agree that "governments should work closely with other organizations, including companies, civil society, academics, and technologists" (Q10-6) to address issues related to privacy and cyber security (ANOVA $F(2, 23864) = 631.17$, $p < .001$, $\eta_p^2 = .050$ and post-hoc tests ($p < .001$)). Regarding whether there should be "new rules about how companies, governments, and other internet users use my data" (Q10-7), individuals from profiles with lower GDP per capita were also significantly more likely to agree (ANOVA $F(2, 23864) = 655.18$, $p < .001$, $\eta_p^2 = .052$ and post-hoc tests ($p < .001$)).

6 Summary of Findings and Discussion

Our findings contribute to the literature in two ways. First, by using data collected from a global survey of individuals across 24 countries we were able to identify three groups based on similarity in online privacy and security attitudes using cluster analysis. Identifying emergent groups based on similarity in privacy preferences has been previously employed in empirical privacy research (Lin et al., 2014; Liu

[2] Ordinal and Likert scales (Likert, 1932) often behave empirically linear and interval in character as proven in several studies (Bishop and Herron, 2015; Carifio and Perla, 2008, 2007; Vickers, 1999). These studies have demonstrated that attitudinal responses from identical participants measured in two different response formats – one continuous and the other ordinal – were highly correlated. We therefore converted ordinal values of the survey responses to an interval scale for the purpose of our analysis.

[3] The ,questions we focus on are Q20-2, Q20-3, Q20-4, Q10-2, Q10-6, Q10-7 from the survey.

et al., 2014; Zhao et al., 2014). However, most of these studies have only identified privacy clusters based on participant samples from a single country. Our work combines cluster analysis with country assignment using dissimilarity measures. Using both approaches in tandem allows us to compare privacy attitudes at a macro-level focusing on each country rather than the individual as the main unit of analysis. As a result, we are able to offer a comparative view of privacy attitudes at the country level using these three profiles. Second, extant literature has focused on cultural variables as the main attribute to country-level differences in privacy; however, we show that the three privacy profiles significantly differ in terms of GDP per capita, linking country-level privacy attitudes with economic standards of living.

6.1 Attitude towards online privacy in relation to GDP per capita

Our findings show that, compared to those living in developed nations, people in countries with lower economic living standards tend to have lower online privacy concerns in regard to personal information being monitored or bought and sold. Such individuals are also relatively less concerned about a general lack of privacy due to having so much personal information about themselves on the web. These findings are aligned with the notion that privacy concern decreases with lower household income (Acquisti and Grossklags, 2006). Over the past few years, developing nations have experienced some of the fastest growth in the number of new internet users and smartphone owners (Anteneh et al., 2015; Poushter, 2016). In fact, while still lagging behind some of the wealthiest economies, developing countries also experienced exponentially sharper increases in the number of people who are newly exposed to online social networking, business transactions, and e-commerce compared to nations with higher GDP per capita (Poushter, 2016). However, increased familiarity in online experiences may not always necessarily imply greater awareness of privacy issues or the ability to protect one's personal information.

Unlike the majority of profile 1 countries where online privacy laws are more comprehensive and have existed for a longer period of time ("Privacy Law," 2017), most developing nations still have nascent or poorly implemented institutional frameworks around data privacy (Anteneh et al., 2015; Nyst, 2012). For example, in all four countries in profile 3 – Pakistan, Nigeria, Kenya, and Tunisia – information privacy laws are very scant and governments rarely enforce protection around corporate or institutional use of people's personal information (Makulilo and Boshe, 2016; Nwankwo, 2016; Nwanne, 2014; Youssef, 2017; Zafar and Ahmad, 2011). Under such conditions, individuals are not only often under-informed about third-party use of their personal information, but also often lack the capacity to protect their data (Anteneh et al., 2015; Borena and Ejigu, 2013; Nyst, 2012). That said, poor legislative protection at the national level, and a resulting lack of awareness around privacy issues, yet increased familiarity in the use of online technology may contribute to a lower sense of inhibition in regard to the privacy risks associated with online technologies.

Furthermore, countries with lower GDP per capita often lag behind much of the world in terms of socio-development indicators (health, education, income, gender equality) on the Human Development Index (Islam, 1995). In such countries, even if there is a wide adoption of technology, people may have different concerns in relation to that technology based on their living standards. For example, 93% of Africans have cell phone service while less than one third of the population have access to flush toilets, 50% live in areas without paved roads, and only 63% have access to piped water (Parke, 2016). Under such conditions, while online privacy issues may still be important, other concerns related to basic necessities may take over greater priority in day-to-day life.

6.2 Attitudes towards government online surveillance and regulation in relation to GDP per capita

Based on our findings, individuals from countries with higher GDP per capita are more reluctant towards government surveillance for the purpose of identifying suspected criminals. Mass government surveillance of online activity is often seen as a threat to democracy and an infringement of basic human right across many nations (Banisar and Davies, 1999; Haggerty and Samatas, 2010; Monahan, 2008). However, governments in emerging economies often "collect and share excessive amounts of personal data in the name of development, security, and modernization of public administration" (Nyst, 2012) without

the proper legislative groundwork to ensure protection around people's personal information. For example, most developed countries like the United States rely on computers to communicate flu data from doctor's offices and emergency rooms to national disease control and prevention centers (Brinkel et al., 2014; Nsubuga et al., 2006; Purvis, 2012). By contrast, in low-income countries "like Kenya where the medical infrastructure isn't developed enough to support a similar nationwide network" (Purvis, 2012), governments rely on people's personal smartphones to collect highly sensitive health information (Brinkel et al., 2014; Nsubuga et al., 2006; Purvis, 2012). Despite the much needed efficiency in terms of cost and time especially for nations that have low resources and capital to manage public health surveillance at a national scale, these circumstances are often rampant with situations where personal data is often shared outside the surveillance system in the process of collecting and storing data (Klingler et al., 2017). Individuals in developing nations who agree to report their data through these surveillance systems are often poorly educated about forgoing informed consent around the use of their personal information (Klingler et al., 2017). As such, in most low-income countries where technology has had some of the most transformative effects in improving humanitarian problems, the perception of benefit may far outweigh perceived privacy risks depending on the context and the role that technology plays.

However, this many not necessarily mean that people in low-income nations are not concerned about the lack of online protection in their countries. In fact, our findings show that individuals in countries with lower GDP per capita are more likely to favour close collaboration between government and other organizations, including companies, civil society, academics and technologists to address cybersecurity threats. Compared to those living in countries with greater economic wealth, these individuals are also significantly more likely to agree that there needs to be new rules about how companies, governments, and other internet users use personal data. Literature shows that individual privacy concerns are associated with perceptions around the effectiveness of privacy policies (Xu et al., 2008) and prevailing privacy social norms (Ciganek and Francia, 2009; Strandburg, 2006) – both of which can widely vary across countries with different levels of economic wealth. While developed nations have instituted online privacy laws across numerous industries at a much earlier stage, developing nations are at the early stages of forming privacy frameworks, with people just starting to become more educated around protecting their personal data (Nyst, 2012).

7 Conclusion and Future Outlook

To the best of our knowledge, no prior work has systematically explored privacy in relation to GDP per capita. In that sense, we contribute to the literature by introducing economic living standards as a lens to examine cross-country privacy. Using a global dataset from the largest world-wide survey on Internet privacy and security concerns, we identified three distinct attitudinal profiles and assigned each country to the best-fitting profile. Our analyses demonstrated significant pairwise differences in GDP per capita based on profile membership as well as attitudinal differences: individuals in profiles with lower GDP per capita had less privacy concerns in relation to information being monitored, bought, or sold, were more tolerant of government surveillance, but were more likely to desire new rules to regulate third-party use of personal data.

However, while our findings showcase significant differences in online privacy and security attitudes based on economic living standards, we are unable to validate causal explanations given the lack of related work on this topic. Through future research we may better understand how and why national economic living standards impact people's privacy concerns.

References

Acquisti, A., Grossklags, J., 2006. Privacy and Rationality, in: Strandburg, K.J., Raicu, D.S. (Eds.), Privacy and Technologies of Identity: A Cross-Disciplinary Conversation. Springer US, pp. 15–29.

Altman, I., 1975. The environment and social behavior: privacy, personal space, territory, crowding. Brooks/Cole Pub. Co.

Anteneh, S., Belanger, F., Borena, B., Ejigu, D., 2015. Conceptualizing Information Privacy Concern in Low-Income Countries: an Ethiopian Language Instrument for Social Network Sites Context. AMCIS 2015 Proc.

Anton, A.I., Earp, J.B., Young, J.D., 2010. How internet users' privacy concerns have evolved since 2002. IEEE Secur. Priv. 8, 21–27. https://doi.org/10.1109/MSP.2010.38

Banisar, D., Davies, S., 1999. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. John Marshall J. Comput. Inf. Law 18.

Bauer, C., Schiffinger, M., 2016. Perceived Risks and Benefits of Online Self-Disclosure: Affected by Culture? A Meta-Analysis of Cultural Differences as Moderators of Privacy Calculus in Person-to-Crowd Settings. Res. Pap.

Bellman, S., Johnson, E.J., Kobrin, S.J., Lohse, G.L., 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. Inf. Soc. Int. J. 20, 313. https://doi.org/10.1080/01972240490507956

Bishop, P.A., Herron, R.L., 2015. Use and Misuse of the Likert Item Responses and Other Ordinal Measures. Int. J. Exerc. Sci. 8, 297–302.

Borena, B., Ejigu, D., 2013. Social Networks and Information Privacy: A Model for Low-income Countries, in: Proceedings of the Nineteenth Americas Conference on Information Systems. Presented at the Americas Conference on Information Systems, Chicago, Illinois.

Bradley, T.L., 1999. Cultural dimensions of Russia: Implications for international companies in a changing economy. Thunderbird Int. Bus. Rev. 41, 49–67. https://doi.org/10.1002/tie.4270410106

Brinkel, J., Krämer, A., Krumkamp, R., May, J., Fobil, J., 2014. Mobile Phone-Based mHealth Approaches for Public Health Surveillance in Sub-Saharan Africa: A Systematic Review. Int. J. Environ. Res. Public. Health 11, 11559–11582. https://doi.org/10.3390/ijerph111111559

Buchanan, T., Paine, C., Joinson, A.N., Reips, U.-D., 2007. Development of measures of online privacy concern and protection for use on the Internet. J. Am. Soc. Inf. Sci. Technol. 58, 157–165. https://doi.org/10.1002/asi.20459

Carifio, J., Perla, R., 2008. Resolving the 50-year debate around using and misusing Likert scales. Med. Educ. 42, 1150–1152. https://doi.org/10.1111/j.1365-2923.2008.03172.x

Carifio, J., Perla, R.J., 2007. Ten common misunderstandings, misconceptions, persistent myths and urban legends about Likert scales and Likert response formats and their antidotes. J. Soc. Sci. 3, 106–116.

Cho, H., Lee, J.-S., 2008. Collaborative Information Seeking in Intercultural Computer-Mediated Communication Groups: Testing the Influence of Social Context Using Social Network Analysis. Commun. Res. 35, 548–573. https://doi.org/10.1177/0093650208315982

Ciganek, A., Francia, G.I., 2009. The Impact of Culture on Global Information Security Regulations. South. Assoc. Inf. Syst. 2009 Proc.
CIGI-Ipsos, 2016 CIGI-Ipsos Global Survey on Internet Security and Trust [WWW Document]. Cent. Int. Gov. Innov. URL https://www.cigionline.org/internet-survey-2016 (accessed 4.20.18).
Dinev, T., Hart, P., 2006. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. Int. J. Electron. Commer. 10, 7–29. https://doi.org/10.2753/JEC1086-4415100201
Dinev, T., Hart, P., 2004. Internet Privacy Concerns and Their Antecedents: Measurement Validity and a Regression Model. Behav. Inf. Technol. 23, 413–422. https://doi.org/10.1080/01449290410001715723
EC, 2011. Attitudes on Data Protection and Electronic Identity in the European Union (No. Special Eurobarometer 359). European Commission, Brussels, Belgium.
Gelman, A. (Ed.), 2004. Bayesian data analysis, 2nd ed. ed, Texts in statistical science. Chapman & Hall/CRC, Boca Raton, Fla.
Groves, R.M., Mathiowetz, N.A., 1984. Computer assisted telephone interviewing: Effects on interviewers and respondents. Public Opin. Q. 48, 356–369.
Haggerty, K.D., Samatas, M., 2010. Surveillance and democracy. Routledge.
Hofstede, G., 2011. Dimensionalizing Cultures: The Hofstede Model in Context. Online Read. Psychol. Cult. 2. https://doi.org/10.9707/2307-0919.1014
Hofstede, G., 2006. What did GLOBE really measure? Researchers' minds versus respondents' minds. J. Int. Bus. Stud. 37, 882–896. https://doi.org/10.1057/palgrave.jibs.8400233
Hofstede, G., 2001. Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations, 2nd edition. ed. SAGE.
Hofstede, G., 1980. Culture and Organizations. Int. Stud. Manag. Organ. 10, 15–41.
Huang, Z., 1998. Extensions to the k-Means Algorithm for Clustering Large Data Sets with Categorical Values. Data Min. Knowl. Discov. 2, 283–304. https://doi.org/10.1023/A:1009769707641
Huang, Z., 1997. A Fast Clustering Algorithm to Cluster Very Large Categorical Data Sets in Data Mining. Presented at the In Research Issues on Data Mining and Knowledge Discovery.
Islam, S., 1995. The human development index and per capita GDP. Appl. Econ. Lett. 2, 166–167. https://doi.org/10.1080/135048595357537
Iyengar, R., 2017. India: Supreme Court privacy ruling puts tech industry on notice.
Kar, I., 2016. The top-country early-adopters of the Internet of Things, ranked. Quartz.
Kaufman, L., Rousseeuw, P.J., 1990. Partitioning Around Medoids (Program PAM), in: Finding Groups in Data. John Wiley & Sons, Inc., pp. 68–125. https://doi.org/10.1002/9780470316801.ch2
Kiiski, S., Pohjola, M., 2002. Cross-country diffusion of the Internet. Inf. Econ. Policy, The New Economy 14, 297–310. https://doi.org/10.1016/S0167-6245(01)00071-3
Klingler, C., Silva, D.S., Schuermann, C., Reis, A.A., Saxena, A., Strech, D., 2017. Ethical issues in public health surveillance: a systematic qualitative review. BMC Public Health 17, 295. https://doi.org/10.1186/s12889-017-4200-4
Kodinariya, T., 2013. Review on determining number of cluster in K-means Clustering.
Krasnova, H., Veltri, N., 2011. Behind the Curtains of Privacy Calculus on Social Networking Sites: The Study of Germany and the USA, in: Wirtschaftinformatik Proceedings 2011.

Lavrakas, P.J., 1987. Telephone survey methods: Sampling, selection, and supervision. Sage Publications, Inc.
Lee, H., Kobsa, A., 2017. Privacy preference modeling and prediction in a simulated campus-wide IoT environment, in: 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom). Presented at the 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 276–285. https://doi.org/10.1109/PERCOM.2017.7917874
Li, Y., Kobsa, A., Knijnenburg, B.P., Carolyn, N.M.-H., 2017. Cross-Cultural Privacy Prediction. Proc. Priv. Enhancing Technol. 2017, 113–132. https://doi.org/10.1515/popets-2017-0019
Likert, R., 1932. A technique for the measurement of attitudes. Arch. Psychol.
Lin, J., Liu, Bin, Sadeh, Norman, Hong, Jason, 2014. Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings, in: Symposium On Usable Privacy and Security (SOUPS 2014). USENIX Association, pp. 199--212.
Liu, B., Lin, J., Sadeh, N., 2014. Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?, in: Proceedings of the 23rd International Conference on World Wide Web, WWW '14. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, pp. 201–212. https://doi.org/10.1145/2566486.2568035
Lowry, P., Cao, J., Everard, A., 2011. Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. J. Manag. Inf. Syst. 27, 163–200. https://doi.org/10.2753/MIS0742-1222270406
Makulilo, A.B., Boshe, P., 2016. Data Protection in Kenya, in: African Data Privacy Laws, Law, Governance and Technology Series. Springer, Cham, pp. 317–335. https://doi.org/10.1007/978-3-319-47317-8_15
Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Nomological Framework. Inf. Syst. Res. 15, 336–355. https://doi.org/10.1287/isre.1040.0032
Marshall, B.A., Cardon, P.W., Norris, D.T., Goreva, N., D'Souza, R., 2008. Social networking websites in India and the United States: A cross-national comparison of online privacy and communication. Issues Inf. Syst. IX 2, 87–94.
McCaskill, A., 2015. Consumers in Developing Countries are More Likely to be "Early Adopters" of New Products (Nielsen Insights).
Milberg, S.J., Burke, S.J., Smith, H.J., Kallman, E.A., 1995. Values, Personal Information, Privacy and Regulatory Approaches. Commun. ACM 38, 65–74. https://doi.org/10.1145/219663.219683
Miles, J., Shevlin, M., 2001. Applying regression and correlation: A guide for students and researchers. Sage.
Monahan, T., 2008. Surveillance As Governance: Social Inequality and the Pursuit of Democratic Surveillance (SSRN Scholarly Paper No. ID 3035028). Social Science Research Network, Rochester, NY.
Naumov, A., Puffer, S., 2000. Measuring Russian Culture using Hofstede's Dimensions. Appl. Psychol. 49, 709–718. https://doi.org/10.1111/1464-0597.00041
Neumann, C., kmodes {klaR}: K-Modes Clustering. CRAN repository.
Nsubuga, P., White, M.E., Thacker, S.B., Anderson, M.A., Blount, S.B., Broome, C.V., Chiller, T.M., Espitia, V., Imtiaz, R., Sosin, D., Stroup, D.F., Tauxe, R.V., Vijayaraghavan, M., Trostle, M., 2006. Public Health Surveillance: A Tool for Targeting and

Monitoring Interventions, in: Jamison, D.T., Breman, J.G., Measham, A.R., Alleyne, G., Claeson, M., Evans, D.B., Jha, P., Mills, A., Musgrove, P. (Eds.), Disease Control Priorities in Developing Countries. World Bank, Washington (DC).
Nwankwo, I.S., 2016. Information Privacy in Nigeria, in: African Data Privacy Laws, Law, Governance and Technology Series. Springer, Cham, pp. 45–76. https://doi.org/10.1007/978-3-319-47317-8_3
Nwanne, B.U., 2014. The Right to Privacy, The New Media and Human Development in Nigeria. J. Mass Commun. Journal. 4, 1–6. https://doi.org/10.4172/2165-7912.1000224
Nyst, C., 2012. Privacy in the developing world: a global research agenda | Privacy International.
Parente, S.L., Prescott, E.C., 1994. Barriers to Technology Adoption and Development. J. Polit. Econ. 102, 298–321. https://doi.org/10.1086/261933
Park, C., Jun, J.-K., 2003. A cross-cultural comparison of Internet buying behavior: Effects of Internet usage, perceived risks, and innovativeness. Int. Mark. Rev. 20, 534–553. https://doi.org/10.1108/02651330310498771
Parke, P., 2016. More Africans have phone service than piped water - CNN [WWW Document]. CNN. URL https://www.cnn.com/2016/01/19/africa/africa-afrobarometer-infrastructure-report/index.html (accessed 4.20.18).
Poushter, J., 2016. Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies. Pew Res. Cent. Glob. Attitudes Proj.
Privacy Law, 2017. . Wikipedia.
Purvis, C., 2012. CDC: Smartphones Could Increase Disease Surveillance In Developing Countries.
Rainie, L., Duggan, M., 2016. Privacy and Information Sharing. Pew Research Center.
Rice, M.E., Harris, G.T., 2005. Comparing Effect Sizes in Follow-Up Studies: ROC Area, Cohen's d, and r. Law Hum. Behav. 29, 615–620. https://doi.org/10.1007/s10979-005-6832-7
Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Q. 20, 167–196. https://doi.org/10.2307/249477
Steenkamp, J.-B.E.., Geyskens, I., 2006. How Country Characteristics Affect the Perceived Value of Web Sites. J. Mark. 70, 136–150. https://doi.org/10.1509/jmkg.70.3.136
Stewart, K.A., Segars, A.H., 2002. An Empirical Examination of the Concern for Information Privacy Instrument. Inf. Syst. Res. 13, 36–49. https://doi.org/10.1287/isre.13.1.36.97
Strandburg, K., 2006. Social Norms, Self Control, and Privacy in the Online World, in: Privacy and Technologies of Identity. Springer US, pp. 31–53.
Survey Methods At Ipsos MORI. Ipsos MORI. URL https://www.ipsos.com/ipsos-mori/en-uk/survey-methods-ipsos-mori (accessed 4.15.18).
Veltri, N., Krasnova, H., Elgarah, W., 2011. Online Disclosure and Privacy Concerns: A Study OF Moroccan and American Facebook Users. AMCIS 2011 Proc. - Submiss.
Vickers, A.J., 1999. Comparison of an ordinal and a continuous outcome measure of muscle soreness. Int. J. Technol. Assess. Health Care 15, 709–716.
Westin, A.F., 2001. How Consumer Privacy and Personalization is Conducted Now and How it Will Be Conducted in 2010 (Invited Keynote), in: Balancing Personalization & Privacy Conference. San Francisco.
Winner, L., 1980. Do Artifacts Have Politics? Daedalus 109, 121–136.
Xu, H., Dinev, T., Smith, H.J., Hart, P., 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. ICIS 2008 Proc. 6.

Youssef, D., 2017. Privacy is Hard to Protect in Tunisia, Thanks to Politics. Glob. Voices Advocacy.

Zafar, F., Ahmad, S., 2011. The challenge of internet rights in Pakistan | GISWatch.

Zhao, C., Jiang, G., 2011. Cultural Differences on Visual Self-presentation Through Social Networking Site Profile Images, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11. ACM, New York, NY, USA, pp. 1129–1132. https://doi.org/10.1145/1978942.1979110

Zhao, Y., Ye, J., Henderson, T., 2014. Privacy-aware location privacy preference recommendations. Presented at the Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), pp. 120–129. https://doi.org/10.4108/icst.mobiquitous.2014.258017