Online Expression, Personal Cybersecurity Costs, and the Specter of Cybercrime

Juhani Rauhala
University of Jyväskylä, Finland

Pasi Tyrväinen
https://orcid.org/0000-0001-7716-3244
University of Jyväskylä, Finland

Nezer Zaidenberg
College of Management Academic Studies, Israel

INTRODUCTION

The UN General Assembly has declared freedom of expression to be a universal human right (UN General Assembly, 1948). As of 2016, the United Nations has resolved that unrestricted access to the Internet is also a human right (UN Human Rights Council, 2016). A commonly accepted benefit of the Internet is that it serves as a platform for free expression. Importantly, political topics are also discussed as well as other topics without socially accepted savoir faire. However, there are potential consequences for users who make controversial or provocative expressions over the Internet from other users and organizations participating in or following the communication (Baroni, 2015; Cassidy, 2017; Jaschik, 2014). Such consequences may also be in the form of illegal doxing or hacking attacks by cybercriminals.

Users' concerns about such consequences may have an inhibiting effect on their Internet usage for free expression. This inhibiting effect may correlate with what users believe and how users behave concerning addressing security and privacy issues of their devices. The inhibiting effect may also correlate with users' attitude toward and perception of the time they spend addressing their devices' security and privacy issues. However, the association between online expression aspects and the perception of time consumption on security aspects is lacking in prior research. Users may be reluctant to express themselves online simply because anonymity costs too much time and effort. That is, the users may be aware of the importance and abundance of tools providing anonymity and may wish to express themselves online but decide that spending time on anonymity is just too much effort. Concern about such consequences may not only have an inhibiting effect on users' use of the Internet for expression but it may also correlate with their desire to purchase personal cybersecurity products and anonymizing services.

Another generally accepted beneficial use of the Internet is as a platform for commerce, which is continuously increasing (Emarketer.com, 2014). At the same time, spending by consumers and businesses on cybersecurity products and services is also increasing (Morgan, 2017). It is reasonable to expect that users purchase a significant proportion of personal cybersecurity software online. It is possible that misgivings of users about the Internet as a platform for free expression may correlate with increased Internet utilization by those same users for commerce in personal cybersecurity products and services. This article explores this somewhat paradoxical relationship given that the Internet is seen as an overall good for humanity. It leads to a focus of this chapter; that is, to the consideration of users' reluctance

DOI: 10.4018/978-1-5225-9715-5.ch067

to express themselves in relation to their attitudes and perceptions regarding the time and money they invest in security. This is relevant to participation in social media and other online expression contexts.

To facilitate research and discussion on this topic, six latent factors are elucidated: three corresponding to a reluctance to self-express online, one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount ("too much") of one's time, and one for time considering device cybersecurity and privacy settings aspects. The sixth factor corresponds to a positive predilection toward personal spending to enhance personal cybersecurity. The correlation among two of these factors is then analyzed. A linear regression of one latent factor against the other and against a demographic factor is also performed.

This chapter presents an overview of related research, followed by a description of a proposed research model. It then establishes the general latent factors. Some results are presented and discussed, followed by a description of future research suggestions, and a conclusion.

BACKGROUND

Previous research has considered implications on free expression and the benefits of free expression. Willingness to express opinions online has been measured in terms of a web forum's view/reply ratio (Shen & Liang, 2015) and by asking users how likely they would be to express their opinions in specified online scenarios using a 0-100% or 0-10 scale (Ho & McLeod, 2008; Stoycheff, 2016). Hayes et al. (2005) established a self-reporting tool consisting of eight five-point Likert questions to measure willingness to self-censor. However, the tool's questions pertain to a general social context and not specifically to self-expression of controversial opinions on the Internet. Attempts to measure a reluctance to express on the Internet or to establish the same as a latent factor are lacking in previous research.

The emerging research of Booth (2017) has raised attention to the issue of freedom of expression and the laws and norms thereof in terms of their relationship to the benefits of ICT on national well-being. However, her research does not consider the relationship between the expression of free speech on aspects of the individual user. Internet communication is largely beyond the territorial control of the nation-state and access to the Internet has been recognized as important to the freedom of expression and to participation in a democracy (Lucchi, 2011). Previous research has established that usage of the Internet for free expression can be a way of circumventing censorship or other hindrances that prevent citizens' freedom of expression in more traditional publishing media, especially in authoritarian regimes (Nadi & Firth, 2004).

Prior research has shown that many states have begun imposing online surveillance upon their citizens by way of legislative acts or other means (Ray & Kaushik, 2017). The research suggests that the ostensible justifications for such surveillance, such as cyberterrorism or cybercrime, are questionable and disproportional to the scope of the surveillance desired by the state. Such surveillance does not directly restrict online expression but it can create hesitation or concern in the user. The user may hesitate to criticize the state or its policies in an online forum due to fear of being surveilled. Many states also impose varying levels of censorship and controls on online expression (Ray & Kaushik, 2017).

Debate and discussions that occur over online forums and social media, such as Twitter and Facebook, are raising the attention to a virtually unlimited array of topics. Importantly, socially controversial topics and political topics are also discussed. Certain organizations consider and evaluate the various threats to the freedom of expression online (Stanton, 2014). In oppressive states, free expression enabled by access to the Internet can be particularly important for advancing human rights (Nadi & Firth, 2004).

However, there are potential consequences for users who make controversial or provocative expressions on the Internet, including a negative reaction from the government (Baroni, 2015; Cooper, 2000; Mony, 2017) and offended individuals (Cassidy, 2017), employers (Jaschik, 2014), and schools (Curtom, 2014). Consequences may also be exacted by vindictive criminal hackers. Cybercrime against individuals has been defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)" (Halder & Jaishankar, 2012). Victims may become a topic for cybercriminal gangs in the Deep Web or the target of doxing. "Revenge hacking" and doxing have caused serious consequences to victims (Branigan, 2011; Dascalescu, 2018). Participating in social media is a form of individual expression and there is some research-in-progress on the effects of perceived security threats on user's social media behavior (Alqubaiti et al., 2016).

Users spend significant time performing self-protective cybersecurity and privacy-related tasks. This time detracts from the amount of time users have available for other preferred activities. For example, when using open WiFi connectivity in a public space or vehicle, spending time connecting to a secure VPN or updating the security software will leave less time for messaging and for checking social media updates. The excess use of time spent waiting can be merely a perception but may still have negative consequences in terms of user experience or perception of the services for which the waiting is done (Dellaert & Kahn, 1999). Another study has been performed to determine how consumers react when web pages of shopping websites take too much time to load (Anonymous, 2010). It found that 70% of respondents reported that they abandon shopping on a site if the site takes more than 10 seconds to load and 35% said they would not return if the loading delays take "too long." On the other hand, the tolerance of users to the amount of time spent waiting will vary according to the individual and the context (Katz & Martin, 1989). During Internet usage, a loading delay may be experienced with most mouse-clicks or screen taps. However, the need to spend time waiting for a security software update process to complete occurs relatively infrequently, e.g. weekly or monthly.

Excessive non-ideal time consumption, therefore, can be said to detract from more desirable activities and may cause a negative perception of offerings associated with waiting. Frustration with excessive time consumption can result in a negative attitude toward, and possibly abandonment of, desirable online content and activities.

Controversial expression in an online communications context is affected by other factors. Such factors include perceived anonymity and familiarity with other online community participants (Luarn & Hsieh, 2014). Luarn and Hsieh studied the expression behavior of users in a laboratory-controlled virtual community. The virtual community simulated different online group communications environments. They found that users were more willing to express controversial opinions when their identities were anonymous or when they were familiar with other members of the community. When users in the study were not anonymous, they were more reluctant to express such opinions. They also found that there was no effect of anonymity or member familiarity on users' willingness to express non-controversial opinions.

Prior research has shown that negative expressions are received differently than neutral or positive ones. Kwon et al. (2013) studied communications and expressions in a messaging context. They examined the acceptability of negative communications. They found that emotional expressions that accompany negative communications were considered much less acceptable than emotional expressions in positive ones. Negative messages by their nature are less welcome. Negative expressions (e.g., unpleasant or aggressive) can result in unwanted consequences. Internet users may be reluctant to express themselves

because of concerns about such consequences. The time they spend on personal cybersecurity issues may further discourage their controversial expressionism.

It is of note that Booth and other researchers utilize the Human Freedom Index (HFI) (Vasquez & Porcnik, 2017). Included in the HFI measures are those that measure freedom of expression. Among those measures are "Laws and Regulations that Influence Media Content," "Political Pressures and Controls on Media Content," and "State Control over Internet Access." The measures of Laws and Regulations that Influence Media Content and Political Pressures and Controls on Media Content could be useful for this study on the condition that they are applied indirectly. That is to say, for example, that an assumption would be that an average user would feel some reluctance to freely express themselves as a result of the laws and controls. This study addresses reluctance more directly in the survey questions, whereas the subset of HFI measures does not measure reluctance to express. The HFI's "expression freedom" measures have not been examined for their relationship to personal cybersecurity spending. In particular, they do not measure concern regarding the consequences of personal free expression and neither have they been analyzed for their relationship to Internet users' attitudes and behaviors toward purchasing personal cybersecurity protections.

There are also studies observing the impact of demographic factors, such as nationality and age, on Internet behaviour that are relevant to this study. Regan, FitzGerald, and Balint (2013) have evaluated attitudes toward information privacy between age groups (specifically generations). Their analysis revealed a trend where younger generations tend to be more concerned than older ones about wiretapping and data privacy. Chen, Hsu, and Lin (2010) determined that consumers with different levels of computer expertise have different preferences for attributes of shopping websites. Research into culture-based differences in perception of risk for online shopping and other tasks has yielded conflicting results (Sims & Xu, 2012). Sims and Xu (2012) found no significant difference between the UK and Chinese shoppers' perceived risk of online shopping despite those shoppers' differing cultural backgrounds. This conclusion was against their expectations and the contradicted results from prior research that showed differences in risk-aversion between the two cultures (Hofstede, 1980).

Sheehan (2002) found that users' education and age correlate with their level of concern about online privacy. Hazari and Brown (2013) studied whether demographic variables can affect Internet users' privacy concerns and, thus, their attitudes toward using social networking sites. In contrast to the results from Sheehan and from Regan, Fitzgerald, and Balint, their research found that age was not correlated with online privacy concerns. Bandyopadhyay (2011) found that factors such as the level of Internet literacy, social awareness, and cultural background affect Internet users' online privacy concerns. He found that among the possible consequences of such concerns is an unwillingness to use the Internet. Liu et al. (2016) applied social exchange theory to examine perceived risks and rewards of individual users' self-disclosure in social media. The authors found that perceived privacy risk can reduce the willingness of social media users to disclose personal information. There does not seem to be existing research on social exchange theory applied to controversial expression by individual users online. Previous work has examined the effect on willingness to disclose information about oneself. Based on previous research, it can be hypothesized that the reluctance to express oneself on the Internet may be connected with concerns about the consequences. Further, reluctance to express oneself may lead to the use of cybersecurity as a means to protect oneself in these cases. However, there seems not to be previous results addressing this hypothesis.

Previous research has attempted to address the monetary and non-monetary costs of consumer-facing cybercrime (Riek & Böhme, 2018). The research focused on cybercrime incidents such as scams and payment fraud. The costs in Riek and Bohme's research are not the costs of the fear of consequences that could result from expressing oneself online. The feared consequences in the RtoEx subfactor of this study are unspecified and general. They may occur in varying forms including, but not limited to, cybercriminal attacks against the user.

The authors believe that it is important to consider the attitudes of users toward free expression on the Internet and possible consequences resulting from users' reluctance to freely express themselves on the Internet.

RESEARCH MODEL

This study proposes six latent factors: three corresponding to a reluctance to self-express online (RtoEx), one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount of one's time (TMT, from "too much time"), and one corresponding to the performance of checking and changing device privacy and security settings (TChS, from "think about and change settings").

The factors are:

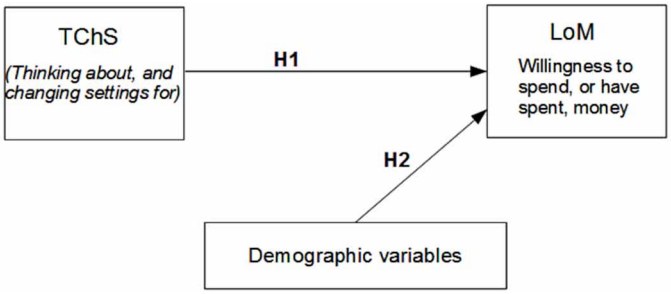
- **Reluctance to Express (RtoEx):** Reluctance to freely self-express online. The reluctance of expressing can be further divided into two factors based on inclusion or exclusion of consequences of the expression, RtoExC and RtoExnonC, respectively.
- **Reluctance to Express When Consequences Mentioned (RtoExC):** Reluctance to Express due to concerns of possible Consequences or safety; The reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.
- **Reluctance to Express When Consequences Not Mentioned (RtoExnonC):** Reluctance to Express when users are not reminded of possible Consequences or safety issues resulting from the expression.
- **Too Much Time (TMT):** The belief that cybersecurity risk amelioration requires excessive usage of one's time
- **Think Change Settings (TChS):** Time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether the time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.
- **Loss of Money (LoM):** Personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

As a demonstration, the authors hypothesize that those users who are conscientious about their online security and privacy will spend both time and money to ensure it. This should be reflected in a significant correlation between TChS and a positive attitude toward purchasing personal cybersecurity products and services (or LoM, for "Loss of Money")(Figure 1).

H1: TChS will be correlated with a positive attitude toward purchasing personal cybersecurity products and services (LoM).

H2: TChS combined with one or more demographic variables will predict LoM.

Figure 1. Latent variables TChS and LoM, and independent demographic variable(s)



Latent Factors and Their Indicators

Each of the latent variables can be derived from sets of indicator questions. Indicator questions for TChS and LoM were included in a survey, and each consisted of responses along a five-point Likert scale from "strongly agree" to "strongly disagree." For data gathering, a survey was administered over the Web to a population composed mainly of Finnish university students and working adults. 191 responses were obtained.

The questions for TMT were as follows: five questions to assess the perception that excessive time has been spent addressing device security and privacy issues and a belief that time spent on device security and privacy aspects has detracted from time intended for other tasks. TChS is established with three questions to assess whether the user has contemplated and checked (and perhaps adjusted) their device's security and privacy settings (available from the authors). Cumulatively, the authors suggest the five "too much time" indicator questions imply that the respondent spends time contemplating and actively addressing security and privacy aspects but tends to feel negative about doing so.

The survey included questions on respondents' behaviors and attitudes regarding personal spending on cybersecurity. Latent variable Loss of Money (LoM) is defined by responses to a set of four indicator questions. The questions for LoM are designed as follows: two questions to ascertain whether the respondent/subject has purchased to enhance his cybersecurity and two questions to ascertain the general attitude of the respondent toward security software purchases (available from the authors). Cumulatively, it is suggested the LoM indicator questions indicate the willingness to buy software products or services that enhance personal cybersecurity.

An Exploratory Factor Analysis with direct oblimin rotation is used to extract latent components from a set of survey questions. The results for TMT, TChS, and LoM confirm three components. Review of the corresponding survey questions indicates that the TMT and TChS responses are differentiated by the mention of security issues detracting time from preferred tasks, or by a belief that addressing security issues takes too much of one's time (Table 1).

A Spearman correlation analysis is performed on the indicator question responses corresponding to TMT (five questions), TChS (three questions), and LoM (four questions). All of the responses within the three respective sets of indicator questions have two-star Spearman correlations with each other (Table 1). Because the indicator questions for the three latent variables have high intercorrelation, the mean scores of the responses were computed and utilized for analysis. SPSS statistical software was used to calculate Pearson correlations between the latent variables as well as the Cronbach's alphas. The Cronbach's alpha values show acceptable reliability between the latent variables' indicators (Table 1).

Table 1. Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor; mean correlations; and Cronbach's alpha

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
TChS	.319**	.485**	.407	.673
TMT	.221**	.772**	.405	.766
LoM	.500**	.863**	.639	.871

Results for TChS and LoM

Analysis of the results (Table 2) for the TChS vs. LoM hypothesis shows a significant correlation, thus H1 is confirmed.

Regression analysis is performed on LoM as the dependent variable against some demographic variables. The analysis shows some correlation with the combination of TChS and age (adjusted R squared = .035, p-value = .013). H2 is therefore valid for age.

When the model is properly applied, hypotheses utilizing the other latent factors may be similarly evaluated.

SOLUTIONS AND RECOMMENDATIONS

From the viewpoint of encouraging open and robust political discourse, governments should ensure the framework and conditions for free expression by their citizens with online regulatory safeguards that correspond to the traditional safeguards in traditional communications media. This could help Internet users feel freer to spend money and time on personal interests instead of diverting spending due to concerns about their online privacy and security. If users would have less reason to be worried about becoming victims of cybercrime, they could spend more time expressing themselves and exploring offerings. In these ways, online merchants could benefit from more confident online consumers, and societies could benefit from the desired online discourse.

The HFI may be enhanced by the inclusion of a measure to assess citizens' reluctance to express legal, but controversial, viewpoints online. Citizens may be reluctant to express such viewpoints despite states' official policies allowing free expression. The concern about consequences resulting from such expression may not necessarily align with states' official policies and the possibility of state-imposed consequences does not necessarily align with states' official policies. The current HFI does not account for citizens' concerns and perceptions of these issues.

In the analysis, some differences between nationalities in the responses were noted. However, further data should be collected. One direction to search for a potential explanation is cultural differences (Hofstede, 1980).

*Table 2. Pearson correlation between LoM and TChS. Two-tailed significance: * to 0.05 level*

	n	Spend time thinking about and changing settings (TChS)
LoM	191	.160*

Better default security and privacy settings could reduce the perceived need for purchasing supplemental personal cybersecurity solutions. This would free up more time and money for users to apply to preferable tasks and transactions. Ideally, users should be confident that their devices have sufficient privacy and security protection "out of the box". Prior research has shown that users' trust in the safeguarding of their privacy and security is positively related to their online purchase intentions (Chen & Barnes, 2007).

FUTURE RESEARCH DIRECTIONS

Applied social exchange theory could be expanded to account for Internet users' reluctance to freely express their thoughts and opinions online. Further research could explore the factors that inhibit users from expressing controversial viewpoints and factors that encourage such expression online.

The indicator questions used in the demonstration study did not examine how, in the case of waiting, the management of time affects the perspective of the person waiting. Examples of such cases could be the users' management of the time spent waiting for a security software update to install; or the content displayed on screen by the software during the update (Hanyang, et al., 2015).

For the TChS vs LoM hypothesis, future research could examine the impact of attitudes toward, and usage of, free and open source personal cybersecurity solutions. Users who believe they can achieve acceptable levels of personal cybersecurity with free tools would not necessarily be purchasing such tools. This could affect the LoM factor and thus the significance of the correlation between LoM and TChS. Regression analysis showed that age affects the TChS vs LoM correlation. Younger users who take time to contemplate their device settings feel more positive about spending money on personal cybersecurity.

This demonstration study did not consider free and open source personal cybersecurity products and tools that are available. Such tools include Tor browser, ClamAV, and free VPN services. Some respondents may have responded negatively to the survey questions regarding spending because they believe that they can achieve sufficient personal cybersecurity without spending money doing so. Future studies could account for such products.

Using the proposed research model and introduced latent variables, research can be performed to determine the effects of some independent variables (e.g., income and ICT expertise) on the relationships between the latent variables. Research can explore the relationship of certain demographic variables to personal cybersecurity spending and to any reluctance to express oneself online. Users could also be surveyed to directly gauge their concern about being victimized by cybercriminals as a result of their expressions. Subject to available survey data, analysis for geographical region clustering and other clusterings could also be performed.

CONCLUSION

While sales of cybersecurity products and services are suitable for the cybersecurity industry, they also indicate the real cybersecurity concerns of Internet users. Many Internet users go online, but may then be reluctant to freely express themselves, spending their time and money to alleviate perceived cybersecurity risks from political vigilantes, cybercriminals, or other entities. This scenario is not the ideal or optimal use of the Internet by society. Future research can investigate methods to encourage free expression online and reduce the perceived risks of such free expression.

In this chapter, an overview of research pertaining to the chapter topic was presented, and a simple research model was proposed. Six latent factors were proposed; three corresponding to a reluctance to self-express online (RtoEx, RtoExC, and RtoExnonC); one corresponding to a belief that handling the security and privacy aspects of one's device requires an excessive amount of one's time, TMT; one for time considering device cybersecurity and privacy settings aspects, TChS; and one for personal cybersecurity spending, LoM. Based on the factor analysis of the responses to some indicator statements, TChS and LoM were established.

A study using two of the latent variable showed a significant correlation between TChS and LoM, thus hypothesis H1 is confirmed. The association transcended nationality. The correlation was significant only when the entire response set was analyzed. Analysis by nationality did not show a significant correlation for any of the three most prominent nationalities of survey respondents. Regression analysis showed that age and TChS are predictors of LoM. Hypothesis H2 is therefore confirmed for age. Younger users who are conscientious about their device privacy and security settings are more likely to spend money on personal security or feel more positively about doing so.

REFERENCES

Alqubaiti, Z., Li, L., & He, J. (2016). The Paradox of Social Media Security: Users' Perceptions versus Behaviors. In Proceedings of the 5th Annual Conference on Research in Information Technology - RIIT '16 (pp. 29–34). Boston: ACM Press. doi:10.1145/2978178.2978187

Anonymous. (2010, January). Keeping online customers. Dealerscope, 52(1), 26. Retrieved from https://search-proquest-com.ezproxy.jyu.fi/docview/218956873?accountid=11774

Bandyopadhyay, S. (2011). Antecedents And Consequences Of Consumers Online Privacy Concerns. *Journal of Business & Economics Research*, *7*(3). doi:10.19030/jber.v7i3.2269

Baroni, D. (2015, July 3). New Zealand Government To Punish Online Trolls With Prison Time. Retrieved from http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time

Booth, R. E. (2017). The Effect of Freedom of Expression and Access to Information on the Relationship between ICTs and the Well-being of Nations. *Proceedings of the 23nd Americas Conference on Information Systems*.

Branigan, S. (2011, July 31). Revenge Hacking. Retrieved May 17, 2019, from Trends in high tech security website: https://sbranigan.wordpress.com/2011/07/31/revenge-hacking/

Cassidy, P. (2017, November 3). Man petrol bombed homes in revenge for Facebook post. STV News. Retrieved from https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/

Chen, Y., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management & Data Systems*, *107*(1), 21–36. doi:10.1108/02635570710719034

Chen, Y.-H., Hsu, I.-C., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of Business Research*, *63*(9–10), 1007–1014. doi:10.1016/j.jbusres.2009.01.023

Cooper, A. K. (2000, July 12). China: Government punishes Internet journalists. Committee to Protect Journalists. Retrieved from https://cpj.org/2000/07/china-government-punishes-internet-journalists.php

Curtom, G. (2014, April 24). Students punished for expressing free speech on Twitter. The Cougar. Retrieved from http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/

Dascalescu, A. (2018, January 3). Doxxing Can Ruin Your life. Here's How (You Can Avoid It). Retrieved May 17, 2019, from Heimdal Security website: https://heimdalsecurity.com/blog/doxxing/#doxxingswatting

Dellaert, B. G. C., & Kahn, B. E. (1999). How tolerable is delay?: Consumers' evaluations of internet web sites after waiting. *Journal of Interactive Marketing*, *13*(1), 41–54. doi:10.1002/(SICI)1520-6653(199924)13:1<41:AID-DIR4>3.0.CO;2-S

Emarketer.com. (2014). Worldwide Ecommerce Sales to Increase Nearly 20% in 2014 - eMarketer. Retrieved November 22, 2017, from https://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039

Halder, D., & Jaishankar, K. (2012). *Cyber Crime and the Victimization of Women: Laws*. Rights and Regulations; doi:10.4018/978-1-60960-830-9

Hayes, A. F., Glynn, C. J., & Shanahan, J. (2005). Validating the Willingness to Self-Censor Scale: Individual Differences in the Effect of the Climate of Opinion on Opinion Expression. *International Journal of Public Opinion Research*, *17*(4), 443–455. doi:10.1093/ijpor/edh072

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, *9*(4), 31–51. doi:10.1080/15536548.2013.10845689

Ho, S. S., & McLeod, D. M. (2008). Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication. *Communication Research*, *35*(2), 190–207. doi:10.1177/0093650207313159

Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values* (1st ed.). Beverly Hills, CA: Sage Publications.

Jaschik, S. (2014, September 15). Interview with professor fired by West Bank university who compares himself to Steven Salaita. Inside Higher Ed. Retrieved from https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita

Katz, K. L., & Martin, B. R. (1989). Improving customer satisfaction through the management of perceptions of waiting. Massachusetts Institute of Technology. Retrieved from http://hdl.handle.net/1721.1/37703

Kwon, O., Kim, C., & Kim, G. (2013). Factors affecting the intensity of emotional expressions in mobile communications. *Online Information Review*, *37*(1), 114–131. doi:10.1108/14684521311311667

Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management*, *53*(1), 53–63. doi:10.1016/j.im.2015.08.006

Luarn, P., & Hsieh, A.-Y. (2014). Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities. *Online Information Review*, *38*(7), 881–895. doi:10.1108/OIR-03-2014-0076

Lucchi, N. (2011). Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. *ARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, *19*(3), 645–678.

Luo, H., Wang, J., Han, X., & Zeng, D. (2015). The impact of filler interface on online users' perceived waiting time. In 2015 12th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1–5). Guangzhou, China: IEEE. 10.1109/ICSSSM.2015.7170198

Mony, S. (2017, November 11). Cambodian Netizens Face New Risks as Government Tightens Online Controls. VOA. Retrieved from https://www.voanews.com/a/cambodian-netizens-new-risks-governmentonline-controls/4111483.html

Morgan, S. (2017). The Cybersecurity Market Report covers the business of cybersecurity, including market sizing and industry forecasts, spending, notable M&A and IPO activity, and more. Retrieved November 22, 2017, from https://cybersecurityventures.com/cybersecurity-market-report/

Nadi, Y., & Firth, L. (2004). The Internet Implication in Expanding Individual Freedom in Authoritarian States. ACIS 2004 Proceedings.

Ray, A., & Kaushik, A. (2017). *State transgression on electronic expression: is it for real?* Information and Computer Security; doi:10.1108/ICS-03-2016-0024

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation (Abingdon)*, *26*(1–2), 81–99. doi:10.1080/13511610.2013.747650

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates†. *Journal of Cybersecurity*, *4*(1). doi:10.1093/cybsec/tyy004

Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, *18*(1), 21–32. doi:10.1080/01972240252818207

Shen, F., & Liang, H. (2015). Cultural Difference, Social Values, or Political Systems? Predicting Willingness to Engage in Online Political Discussion in 75 Societies. *International Journal of Public Opinion Research*, *27*(1), 111–124. doi:10.1093/ijpor/edu012

Sims, J., & Xu, L. (2012). Perceived Risk of Online Shopping: Differences Between the UK and China. In UK Academy for Information Systems Conference Proceedings (Vol. 25). Academic Press.

Stanton, L. (2014, August 18). Effect of "right to be forgotten" on free expression sparks debate. Cybersecurity Policy Report.

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296–311. doi:10.1177/1077699016630255

UN General Assembly. (1948). Universal Declaration of Human Rights. Retrieved from https://www.un.org/en/universal-declaration-human-rights/index.html

UN Human Rights Council. (2016). Resolution on the promotion, protection and enjoyment of human rights on the Internet. Retrieved from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Vasquez, I., & Porcnik, T. (2017). *The Human Freedom Index 2017: A Global Measurement of Personal, Civil, and Economic Freedom*. Washington, DC: Cato Institute, Fraser Institute, and the Friedrich Naumann Foundation for Freedom.

ADDITIONAL READING

Camulli, E. (2012, November 28). Customer Experience Frustration Points and Their Consequences. CMSWire. Retrieved from https://www.cmswire.com/cms/customer-experience/customer-experience-frustration-points-and-their-consequences-018455.php

Chua, C., Rose, G., Khoo, H. M., & Straub, D. (2005). Technological Impediments to B2C Electronic Commerce: An Update. *Communications of the Association for Information Systems*, 16.

Cushman, T. (2016). The Fate of Freedom of Expression in Liberal Democracies. *Society*, *53*(4), 348–351. doi:10.100712115-016-0047-z

Hayes, A. F. (2005). Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research. *International Journal of Public Opinion Research*, *17*(3), 298–323. doi:10.1093/ijpor/edh073

Hong, S.-B., Zalesky, A., Cocchi, L., Fornito, A., Choi, E.-J., Kim, H.-H., ... Yi, S.-H. (2013). Decreased Functional Brain Connectivity in Adolescents with Internet Addiction. *PLoS One*, *8*(2), e57831. doi:10.1371/journal.pone.0057831

Kraut, R. E., Patterson, M., Lundmark, V., Kiesler, S., Mukhopadhyay, T., & Scherlis, W. (1998). Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being? *The American Psychologist*, *53*(9), 1017–1031. doi:10.1037/0003-066X.53.9.1017

Rose, G. M., Evaristo, R., & Straub, D. (2003). Culture and consumer responses to web download time: A four-continent study of mono and polychronism. *IEEE Transactions on Engineering Management*, *50*(1), 31–44. doi:10.1109/TEM.2002.808262

Ryan, G., & Valverde, M. (2005). Waiting for service on the internet: Defining the phenomenon and identifying the situations. *Internet Research*, *15*(2), 220–240. doi:10.1108/10662240510590379

Strebel, J., O'Donnell, K., & Myers, J. G. (2004). Exploring the connection between frustration and consumer choice behavior in a dynamic decision environment. *Psychology and Marketing*, *21*(12), 1059–1076. doi:10.1002/mar.20037

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. doi:10.1016/j.cose.2016.02.009

KEY TERMS AND DEFINITIONS

HFI: Human freedom index; a numerical measure of the personal and economic freedom available in a country. It is measured annually. The HFI is determined from an evaluation of over 70 different indicators for each measured country.

LoM: Loss of money; personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

RtoEx: Reluctance to express; the reluctance to freely express oneself online or on the internet.

RtoExC: Reluctance to express due to concerns of possible consequences or safety; the reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.

RtoExnonC: Reluctance to express when users are not reminded of possible consequences or safety issues resulting from the expression.

Social Exchange Theory: A behavioral theory that seeks to explain the interaction between a person and another person or entity. Its fundamental proposition is that the interaction is influenced by the person's evaluation of the interaction's risks versus rewards.

TChS: Thinking about and changing settings; time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.

TMT: Too much time; the belief that cybersecurity risk amelioration requires excessive usage of one's time.