CYBERSECURITY PERSPECTIVES

TRUST AND MISTRUST: ARE REGULATIONS AND STANDARDS ADDRESSING BOTH ELEMENTS FOR ECOMMERCE TO THRIVE?

Johnny Guimaraes

Paper 1 | August 2019

Suggested Citation:

Guimaraes, J. (2019). Trust and Mistrust: Are regulations and standards addressing both elements for eCommerce to thrive? *AICL Cybersecurity Perspectives*, Paper 1, accessed on August 18, 2019, https://www.americascyber.org/cyberperspectives.

ABSTRACT

Although e-commerce has grown steadily over the last decade, the growth rate in terms of overall retail volume has fallen short of its potential. In contrast, online health portals have received greater consumer acceptance overall. Much of the research on e-commerce adoption indicates that consumer information privacy concerns are the leading reason behind the low e-commerce adoption rate, which stood at 9.1% of overall retail dollar volume in the first quarter 2018. Two of the underlying issues regarding information privacy concerns is consumer trust and distrust. In order for e-commerce to grow, stronger laws and industry standards need to be implemented that contain mechanisms to address information privacy and carry penalties for their infraction. In order to be effective, the mechanisms in information data privacy laws and standards need to address consumer trust and distrust. We review current U.S. information privacy regulations and industry standards to discuss the need for addressing trust and distrust elements.

1. INTRODUCTION

A Pew Research study published by Rainie and Cohn (2014), found that 84% of United States (U.S.) households own a computer and of these households, 70% also have broadband connection to the internet. In this same study, it was also determined that 87% of U.S. adults indicated that they use the internet, either at home or at work. With the proliferation of computers and internet access, many industries have expanded their presence onto the internet and many new "ONLINE-ONLY" companies and organizations have come into existence. The movement to online business has created a new dynamic called business to consumer electronic commerce (B2C e-commerce).

Many U.S. industries have migrated part or all of their services onto the Internet to increase customer convenience and enhance customer service. To a small degree, online consumer acceptance of B2C e-commerce has increased steadily, albeit slowly over the last decade. The U.S. Census Bureau (2018) reports that the e-commerce percentage of total U.S. retail sales grew from 3.6% in the first quarter 2008 to 9.1% in the third quarter of 2017, or a mere 6% during the nice year period. As of the Census Bureau report, retail e-commerce in the U.S. remains below 10% of overall retail volume. Based on the slow adoption and the low volume rates, the growth rate of B2C e-commerce in terms of overall consumer retail expenditure is failing to meet its potential.

In contrast, consumer electronic health record (EHR) portals have experienced greater consumer adoption success. Based on a survey of 500 patients by HealthMine, Heath (2016) reports that 55 % use their EHR access to stay informed of their clinical data and 22 % of consumers use EHR data to make medical decisions. These adoption rates have occurred over a similar 9 year period beginning when the Health Information Technology for Economic and Clinical Health (HITECH) Act that was signed into law on February 17, 2009.

The reasons behind B2C e-commerce's lag in overall U.S. retail sales has been the topic of much research over the last decade. Some researchers have indicated that consumer privacy concerns have held back the growth of e-commerce adoption (Belanger, et. al, 2002; Dinev and Hart, 2006; Pavlou et. al, 2007) and the primary, underlying factor for these privacy concerns is the lack of consumer trust that the organizations collecting their personal information will adequately protect and keep their data private.

If privacy concerns are keeping consumers from embracing B2C e-commerce, why are these concerns not likewise a factor for consumer adoption of EHR consumer portals? This paper will attempt to address this question by examining the potential drivers that are impacting consumer privacy concerns from a trust and distrust motivational standpoint.

2. DEFINITION OF INFORMATION PRIVACY

Privacy has many different meanings and contexts. The most basic of these definitions provided by Warren and Brandeis (1890) is privacy being the fundamental right to be left alone. In today's information and data environment with personal information being stored in the "cloud", the proliferation of mobile devices that contain large amounts of user information, and the phenomenon of social media, the definition provided by Warren and Brandeis (1890) may be considered far too simplistic for today's technology driven world.

Information security researchers such as Stone et al. (1983) and Belanger et al. (2002) define information privacy as the ability to control personal information about one's self. The issue of control over one's personal information also contributes to the underlying issue of secondary use of data where the original collector of the information shares it with another person or organization without the knowledge or consent of the consumer who provided the information (Belanger et al. 2002; Culnan and Armstrong, 1999), drawing upon the feelings of trust and distrust. Belanger et al. (2002) also points out that such privacy concerns are having an impact on e-commerce adoption, which the U.S. Census Bureau (2018) figures seem to support.

In order to address the issue of privacy, we must first have a clear idea of what privacy means to us personally and to our organizations. Without a clear contextual definition of information privacy, an organization's privacy program may become ineffective or even fail. Therefore, for purposes of this paper, we will consider information privacy to be *the ability for an individual to control their personal information provided to a Web vendor*. It will be from this definition of information privacy that this paper will draw upon to examine the roles that trust and distrust has on consumer on-line behavior.

3. PRIVACY PROBLEM

The loss of control over freely submitted personal information during an e-commerce transaction is an information privacy concern for many U.S. consumers, having a negative impact on e-commerce adoption (Belanger et al., 2002). The consumer's fear of losing control of their personal information is a product of trust that the Web vendor will honor consumer information privacy.

Consumer trust has been a seminal information privacy research topic for some time. Belanger et al. (2002) examined the role of trust as a construct in addressing consumer information privacy concerns. Specifically, Belanger et al. (2002) examined the role that privacy seals, privacy statements, third party security seals, and website security features have on consumer trust. The study's findings indicate that Website security features, not privacy seals or statements, have the most significant impact on consumer trust and privacy concerns. Studies conducted by other researchers have led to similar conclusions that privacy seals have little impact on consumer trust (Bandyopadhyay, 2011; Schwaig, 2006; Hui, 2007). The reasons for these findings range from consumer ignorance of what privacy seals signify to the voluntary and non-enforcement nature of privacy seals.

Liu et al. (2005) tested a theoretical model that accounted for a consumer's perception of online privacy and its impact on their trust level in a Web vendor's online site. The study

used a laboratory approach to test participant reaction to a "high security" Website. The Website contained the dimensions of privacy notices, privacy seals, security notices, and access to the participant's information. The study also tested participant reaction to a "low security" Website that did not include any of the privacy dimensions. The results indicated that consumer trust was determined to be an important intermediary variable that influences behavioral intentions to perform an online transaction.

Other studies have looked to consumer beliefs and behavioral intentions to help explain when the decision to share or not share personal information online is made. Dinev and Hart (2006) determined that there is a cumulative influence between Internet trust and *Personal Internet Interest* that can potentially override privacy risk perceptions.

Based on the literature, the relationship between information privacy concerns and a consumer's use of e-commerce is in part driven by trust. The research examines trust based on voluntary rules and standards implemented by Web vendors or on user beliefs and privacy attitudes. Absent from the discussion is the role government regulations and industry standards have on consumer trust and distrust.

4. NOVEL APPROACH

With information privacy concerns being one of the main issues holding back e-commerce in the U.S., researchers have been studying ways in which to address these concerns to potentially unlock e-commerce's potential. One of the main underlying issues with consumers is trust that the Web vendor will safeguard their private information and not sell or disclose this information with other third parties.

4.1 Privacy Research

Research on consumer trust within the context of information privacy has been an ongoing subject that has led to the emergence of distrust as a distinct element to factor into the

information privacy concern equation (Andrade, et al., 2012; Benamati & Fuller, 2006; Bigley & Pearce, 1998; Lowry, et. al., 2015). Perhaps the most convincing aspect to trust and distrust being distinct elements lies in recent neuroscience research. Tejay and Mohammed (2017), through the use of neuroscience, established the role distrust has on the privacy calculus as a distinct factor to trust. Dimoka (2010) used functional neuroimaging (fMRI) to study the distinct locations and effects within the human brain that processes trust and distrust signals.

The findings from Dimoka's (2010) study demonstrated that trust is associated with the reward, prediction and uncertainty section of the brain, and distrust is associated with the intense emotions and fear for loss section of the brain. From a neurophysiological standpoint, these studies (Dimoka, 2010; Tejay and Mohammed, 2017) support the argument that trust and distrust are two distinct elements that need to be factored into the information privacy paradigm.

Whereas the definition of trust within the information privacy and security context is more readily agreed upon, the opposite is true for distrust. Trust is generally defined within the e-commerce context as the buyer's intentions to accept vulnerability based on beliefs that the transaction will meet the buyer's confident expectations (Pavlou et al., 2007; Mayer et al. 1995). Agreement on a definition of distrust, however, has been more elusive.

McKnight and Chervany (2001) provide a detailed analysis of conceptual definitions for distrust across the literature. They summarize their review by indicating that distrust differs from trust qualitatively in terms of the depth of emotion behind it. McKnight and Chervany (2001) state that distrust is "hot or even frenzied" because it may be caused by feelings of betrayal, paranoia, or victimization. Marsh and Dibben (2005) propose that distrust is a measure where the trustor believes that the trustee will actively work against them in a given situation. In their study, Marsh and Dibben (2005) indicate that distrust is at least as important as trust in e-commerce.

McKnight et al. (2003) concluded that the disposition to distrust is well suited to address

issues of high risk, whereas the disposition to trust is suited to low risk issues. They define high risk issues to include perceptions that a Website is risky and the resulting willingness to depend on an unknown Web vendor in terms of the risk. McKnight et al. (2003) further postulates that consumers distrust the Web because safeguards established with brick and mortar commerce are missing on the Web. In other words, there is no physical location for the consumer to establish the legitimacy of the business or inventory to touch and try.

We argue that in order to increase e-commerce adoption, laws and industry standards must be strengthened to include mechanisms that directly address consumer information privacy concerns, specifically in the areas of trust and distrust. If both of these elements are not adequately addressed, e-commerce in the U.S. will continue to underperform.

4.2 Privacy Laws

Privacy laws in the United States (U.S.) are at best fragmented. The U.S. does not have a comprehensive national law that regulates the collection and use of consumer personal information. In Ieuan Jolly's (2017) legal review of information privacy legislation, the author writes that information privacy in the U.S. is a hodgepodge mixture of federal and state laws and regulations that can overlap, link together, and contradict one another.

In contrast, the European Union (EU) enacted the General Data Protection Regulation (GDPR) on May 25, 2018. GDPR is a unified, comprehensive data and information privacy law applicable across all industries and governments in the EU to protect the data privacy of EU citizens. A key element of GDPR is its extended jurisdiction since it applies to all companies processing personal data of EU citizens regardless of the company's location. GDPR provides unified requirements for every industry to follow and it gives EU citizens control on how their personal data can be used by those who collect their information. GDPR also has strong enforcement, compliance, and penalty components.

The effectiveness of GDPR and its effect on EU citizens' trust and distrust attitudes and

perceptions concerning their information security remains to be seen. The key point here is that GDPR has eliminated a confusing and fragmented system and replaced it with one comprehensive approach to address information privacy and security.

In lieu of a comprehensive information privacy law, many U.S. Web vendors indicate their compliance with the Fair Information Practice Principles (FIPPS). These principles provide a guide for an organization's use of consumer personal information in connection with business transactions and activities. The FIPPS principles include: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress. These principles are purely voluntary and not a law that must be followed, and thus not enforceable. The viability of self-regulation mechanisms over disclosure of privacy policies, however, has been questioned in research which indicates little impact on consumer trust of electronic transactions (Dinev and Hart, 2006).

The U.S. government enacted the Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) in 1914 as a consumer protection law to address unfair or deceptive practices which has been applied to online privacy and data security policies. Although these standards and regulations attempt to address consumer information privacy concerns, they have not demonstrated themselves to be effective in addressing consumer trust and distrust concerns.

In contrast to e-commerce, U.S. healthcare is regulated through HIPAA (Health Insurance Portability and Accountability Act of 1996) legislation that provides data privacy and security provisions for the safeguarding of patient medical information. As stated earlier, consumer use of online health portals, although not overwhelming, has a higher utilization rate than retail e-commerce. The disparity between e-commerce and online health portal usage presents a unique question of what degree does government regulations play in consumer trust to adopt increased use of online transaction mechanisms.

In order to increase e-commerce in the U.S., stronger laws are needed to build consumer trust in order to address their information privacy concerns and minimize distrust. Two elements associated with strong laws are (1) mechanisms that address information privacy

protection, and (2) penalties that punish individuals and organizations that willfully violate the law's provisions.

5. CONCLUSION

E-commerce has many drivers, the foundation of which is consumer trust and distrust. The underperformance of e-commerce adoption seems to indicate that consumers have concerns accepting this commerce platform. Current U.S. laws and regulations are fragmented which lead to confusion and gaps in practice and enforcement and impact consumer confidence in a negative manner.

Without a unified, comprehensive information privacy and security regulation across all industries can follow, companies must implement voluntary self-regulation practices to gain consumer confidence. However, consumers see this practice for what it is, and in light of ongoing security breaches and news headlines about the misuse of information, consumer confidence of e-commerce is lower than it should be. For the practitioner, the elements of trust and distrust must be addressed concurrently to maximize their e-commerce presence. This may require multiple approaches to address consumer comfort in making e-transactions on the Internet.

This paper addresses the role of trust and distrust with respect to consumer confidence and introduces a potential mitigating element of a national comprehensive information privacy and security law for the U.S. While more research is needed in this area, the EU's implementation of GDPR provides researchers with an excellent platform for ongoing study on how that national law influences consumers intention and use of e-commerce.

REFERENCES

Andrade, A. A., Lopes, V. V., & Novais, A. Q. (2012). Quantifying the Impact on Distrust of E-commerce Trust Factors: A Non-parametric Study. *Proceedings from the 7th International Conference for Internet Technology and Secured Transactions.*

Bandyopadhyay, S. (2011). Antecedents and Consequences of Consumers Online Privacy Concerns. *Journal of Business & Economics Research*, *7*(3), 41–48.

Belanger, F., Hiller, J. S., and Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, *11*, 245–270.

Benamati, J., Serva, M. A., & Fuller, M. A. (2006). Are trust and distrust distinct constructs? An empirical study of the effects of trust and distrust among online banking users. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 6*.

Bigley, G. A., & Pearce, J. L. (1998). Straining for Shared Meaning in Organization Science: Problems of Trust and Distrust. *The Academy of Management Review*, *23*(3), 405-421.

Culnan, M. J., and Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1), 104–115.

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly, 34*(2), 373–396.

Dinev, T., and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Heath, S. (2016, May 2). *Only 20% of Patients Use EHR Access to Make Medical Decisions*. Retrieved from https://patientengagementhit.com/news/only-20-of- patients-use-ehr-access-to-make-medical-decisions/.

Hui, K. L., Teo, H. H., and Lee, S.-Y. L. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly, 31*(1), 19–33.

Jolly, I., Loeb, and Loeb (2017, July 1). *Data protection in the United States*: *Overview*. Retrieved from https://content.next.westlaw.com/6-502-0467.

Liu, C., Marchewka, J. T., Lu, J., and Yu, C. S. (2005). Beyond concern - a privacy-trust-behavioral intention model of electronic commerce. *Information and Management, 42*(2), 289–304.

Lowry, P. B., Schuetzler, R. M., Giboney, J. S., & Gregory, T. A. (2015). Is Trust Always Better than Distrust? The Potential Value of Distrust in Newer Virtual Teams Engaged in Short-term Decision-Making. *Information Systems and Quantitative Analysis*, *43*, 1-41.

Marsh, S., and Dibben, M. R. (2005). Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side. *Proceedings of the 3rd International Conference, iTrust*, 17–33.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review, 20*(3), 709–734.

McKnight, D. H., and Chervany, N. (2001). While Trust is Cool and Collected, Distrust is Fiery and Frenzied: A Model of Distrust Concepts. *Proceedings of 7th Americas Conference on Information Systems*, 171.

McKnight, H., Kacmar, C., and Choudhury, V. (2003). Whoops... did I use the wrong concept to predict e-commerce trust? Modeling the risk-related effects of trust versus distrust concepts. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, 1–10.

Pavlou, P. A., Liang, H., and Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principle - agent perspective. *MIS Quarterly, 31*(1), 105–136.

Cohn, D. (2014, September 19). *Census: Computer Ownership, Internet Connection Varies Widely across U.S.* Retrieved from https://www.pewresearch.org/fact-tank/2014/09/19/census-computer-ownership-internet-connection-varies-widely-across-u-s.

Schwaig, K. S., Kane, G. C., and Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information and Management, 43*(7), 805–820.

Stone, E. F., Gueutal, H. G., Gardner, D. G., and McClure, S. (1983). A Field Experiment Comparing Information Privacy Values, Beliefs and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology, 68*(3), 459–468.

Tejay, G., and Mohammed, Z. (2017). Understanding Privacy-Related Decisions Through Individuals' Neural Disposition: A Neuroscience Study. *Proceedings of 2017 IFIP Dewald Roode Workshop on Information Security and Privacy*.

U.S. Census Bureau. (2018, February 16). *The 4th Quarter 2017 Retail E-Commerce Sales Report (Report No. CB18-21).* Retrieved from https://www.census.gov/retail/index.html.

Warren, S., and Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

AUTHOR BIOGRAPHY

Johnny Guimaraes is an IT and financial professional with over 28 years of experience. He has worked in IT security and operations, data analytics, accounting, and compliance. Johnny has held managerial and executive positions in Fortune 500 corporations, municipal /county/state government, and non-profit agencies. He holds the CIA, CGFM, CFE, CISA, CISM certifications and is a Certified John Maxwell Team Member on Leadership. Johnny received his undergraduate degree in Finance from the University of Florida, and Master of Business Administration and Master of Science in Information Management from Nova Southeastern University. Johnny also has 35 credit hours in the Master of Accounting program from Florida International University and is currently pursuing his doctorate degree in information security from St. Thomas University. Johnny currently serves as the Vice President of Information Technology and Data Analytics for the South Florida Behavioral Health Network, Inc. in Miami, Florida.