How Do We Get People to Use Digital Identity?

1 Introduction

Canada's economy is undergoing a digital transformation, and many industries, organizations, and businesses are relying more and more on online interaction with their customers. Unprecedented events are now accelerating this transformation, such as the COVID-19 pandemic, which requires physical distancing and travel restrictions. Recent developments in mobile devices, mobile apps, and cloud-based services also promise to transform the way entire industries do business. People currently shop online, bank online, and access government services online. But why can't they do more? Why can't people apply for a passport online; renew their driver's license online; or vote from home?

Simply put, some systems can't confirm with enough confidence that the people who request service are the ones who they claim to be. Although we have been experiencing a radical digital transformation in the current decade, we still mainly prove our identity physically, using paper or plastic documents. This reliance on physical identity is becoming a significant barrier to innovation. We need to create a highly secure, ubiquitous and convenient digital identity and authentication method to enable people to identify themselves and receive services online.

Developing a digital identity system will have many benefits:

- Unlocking new and enhanced experiences for citizens as they interact with government and businesses [1].
- Creating new markets and lines of business, better customer experiences, and higher protection against fraud [2].
- Enabling governments to provide citizens with greater accessibility and simplify interactions at a lower cost [2].
- Allowing Canadians to prove their identity to access health data and consent to record sharing, which significantly reduces time and costs associated with referrals, the release of information, and general patient administration [3].

However, the implementation of a successful identity system is complicated and highly sensitive to situational, operational and cultural factors. Identity is both deeply personal and foundational to essential matters like wealth and access to services. As a result, widespread adoption by individuals and organizations will depend not only on the technical capabilities of a particular solution, but also (and likely even more so) on the individual acceptance of the solution provided.

The first step in developing such an infrastructure is to see how people feel about this new technology:

- What factors are influential in people's acceptance to disclose their confidential identity on a digital identity system?
- What is their attitude toward privacy in such a system?
- Who are the early adopters of this system?
- And what individual characteristics are essential in predicting the early adopters?

This paper explores these questions.

2 What is Digital ID?

Digital identity is a relatively new concept with various definitions. Some refer to digital identity as a means to support digital 'onboarding,' and some consider it as something more significant such as a digital equivalent of a passport or national identity scheme. Even the U.S. National Institute of Science and Technology (NIST), in its Guidelines, points out that: "Without context, it is difficult to land on a single definition that satisfies all." However, there are some broader definitions:

Digital ID and Authentication Council of Canada (DIACC) [4]: Digital identity (ID) is a set of attributes that links a personal entity with their online interactions by using trusted sources.

Mastercard [1]: Digital ID is a collage of up-to-date, high-fidelity digital data that defines an individual, which is dynamic, multipurpose, and reusable including name, date of birth, address, biometrics (e.g., fingerprint, face, voice), attributes (e.g., passport number, social insurance number), certificates (e.g., university degree), and dynamic data from users interactions with financial institutions, mobile and retailers.

The Financial Action Task Force (FATF) [5]: Digital ID systems use electronic means to assert and prove a person's official identity online (digital) and/or in-person environments at various assurance levels. According to FATF, official identity is the specification of a unique natural person that is based on characteristics (attributes or identifiers) of the person that establishes a person's uniqueness in the population or particular context(s) and is recognized by the state for regulatory and other official purposes.

The core concept in all definitions is that **digital identity establishes trust for online transactions.** Different entities can be responsible for the operation of a digital identity system (Figure 1). The participants include a party who asks for a user identity (i.e., relying parties), a person who asserts his or her identity (i.e., users), and a party who knows and verifies the identity of the person (i.e., identity provider). Users also need a digital identity service provider (i.e., a governance body) who orchestrates the operation of all players, creates the necessary tools that connect the parties online and enables users to control and present their identity [1]. Another possible role in this ecosystem is a trust provider [1]. The trust provider is an organization such as a financial institution that has a preexisting relationship of trust with users and can act as a bridge to a digital identity service. It might be the user's bank, for example. The trust provider can also supply the tools and service connectivity for users to register for, use, and manage their digital identities [1].

Many new identity systems are under development around the world in response to the need for digital identity and new technology capabilities. However, not all have been successful [6]. Implementing a successful identity system is delicate and highly sensitive to situational, operational and cultural factors. The highest-level considerations in the development of an identity system are the user group [6]. When designing and configuring identity systems, one crucial question which should be answered is which user groups do this system serve and what characteristics will affect acceptance by these user groups [6]. A reusable digital identity service is impossible without user engagement. Thus, identifying and understanding the factors that influence users' trust in a new identity system is necessary. Once we recognize these factors, we can segment users, identify the early adopters, and develop an effective digital identity system.

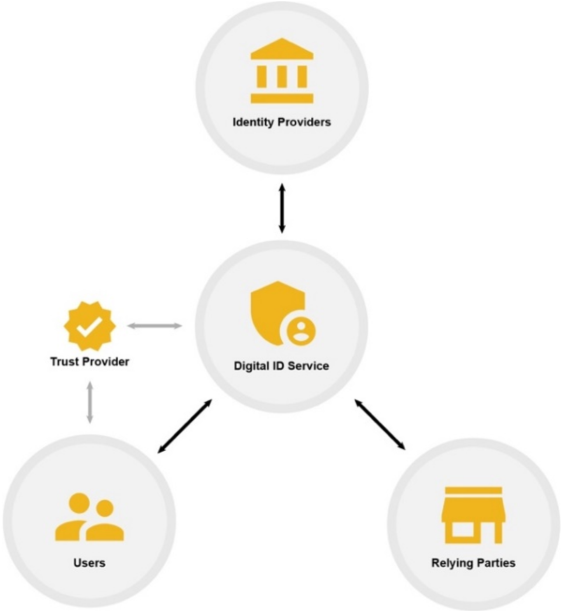

Figure 1: Digital Identity Service Ecosystem

3 What is Trust?

Trust is a complex notion that is thought of differently depending on the discipline [7], [8]. For example, psychologists consider trust to be a personal attribute [9]. Social psychologists view trust as an interpersonal phenomenon [10]. Technologists define trust with respect to technology adoption. While numerous interpretations of trust exist, there are three universal elements necessary for trust to occur [11]-[13]:

- Two parties must exist to develop trust (trustor and trustee)
- Risk and exposure to unknown must be present (trust occurs only in an uncertain situation)
- Trust is sensitive to context (many subjective personal and situational factors influence trust)

For example, while engaging in an online transaction, users, as trustors, find themselves in a risky situation where they communicate their needs to another public or private organization through an online platform and submit their personal and private information. In these situations, users expect the platform and the provider of the platform to be reliable and fulfil their request in an honest and professional manner. Therefore, online trust can be defined as the confident acceptance of risk and exposure to the unknown in an online situation when one's vulnerabilities will not be exploited [13]-[15]. Although the online environment includes more uncertainty than face-to-face situations, researchers believe that the nature of trust in face-to-face and online situations are not fundamentally different. For example, Corritore et al. [16] argue that the findings of studies on trust in offline settings are applicable to trust in online environments. Shankar et al. (2002) specify that the only difference between offline and online trust is in terms of their objects of trust. The object of trust in an offline context is typically a person or an organization, whereas, in an online context, the technology and the organization deploying the technology are the objects of trust [15].

Online transactions are faceless and intangible, and associated with higher uncertainty and risk; hence, the wider acceptance depends not only on the benefits offered by the online technology, but also on users' trust in the technology, and the organizations offering the technology [15]. Considerable research has been done on the antecedents of trust in online technologies. According to these studies, users' trust depends not only on their evaluation of the technology and the institution providing the technology, but also on some of their own personal values and characteristics. In this paper, we reviewed the relevant literature to identify potential factors that may influence users' trust in and adoption of the digital ID.

4 Antecedents of Trust

Antecedents of trust are the factors that make someone more likely to put their trust in a given situation. Our findings indicate that there are several trust-related determinants in the context of user interaction with and adoption of online technologies, including:

- Factors related to the technology itself;
- Factors related to the institutional parties offering and supporting the technology;
- Personal characteristics of users.

The discussion of the different antecedents of trust in online transactions in this review is based on the results of different academic research or industrial reports in the context of e-commerce, e-government and e-health. Table 1 provides a summary of all antecedents of trust discussed in this review.

Technological Factors
Usability
Reliability
Ease of Use
Appearance & Graphical Characteristics
Customization & Personalization
Technological Security Measures
Transparent Data Collection, Usage, & Process
Visibility of Third-Party Access to Data
Control
Institutional Factors
Reputation of a Technology Provider
Organization Size
Third-Party Guarantee
Security Certificates from Third Parties
Regulation & Standards
Information & Support
Promoting the Benefits of Technology
Personal Factors
User Experience & Knowledge
Innovativeness
Self-Efficacy
Perceived Risk
Convenience Orientation
Demographic Variables
Need for Uniqueness
Prestige Orientation

Table 1: Possible Antecedents of Trust in Digital Identity Services

4.1 Technological Factors

4.1.1 Technology Performance

The degree to which users believe that using a technology will improve and enhance their performance, which refers to as *usability*, is the first key factor in adopting and using that technology [17]-[19], particularly in settings where performance is key. In other words, if a new technology is not perceived as enhancing performance, increasing effectiveness, and simplifying tasks, it will not receive wide users' acceptance. The user's awareness of the benefits provided by the technology is a significant factor, and institutions' performance in promoting, supporting and providing information about the introduced technology plays an important role.

Reliability, or the consistent, and accurate performance of new technologies, is the second factor that positively correlates with users' trust [20]-[22]. Products and services with good reliability tend to be perceived as more trustworthy by users [23]. In order to enhance users' trust, the actual performance of a product or service should meet the promised performance [17], [24]. In this regard, the first users' impression of technology is significantly important [25]. Consistent and reliable operation is more important for technologies such as digital ID, which is users might need at any time and in any location.

The other performance-related factor identified in prior research as a possible driver of adopting new technologies or applications is *ease of use* [26]. A new service or product should be as simple as possible to use [17], and any complexity should be hidden from the users as far as possible [27]. Many empirical studies have shown the positive influence of perceived ease of use on users' acceptance of e-commerce services [27]-[30]. Flavian et al. [27], for example, argue that online services that are hard to use may result in technical errors that decrease users' feelings of trust and could cause them to use the service less. When users are able to understand the procedures and what is going on while they are using a service, there is a less associated risk, and it seems more reliable [31].

In the case of digital ID, as well, users want a frictionless experience and do not have the patience for a cumbersome authentication process [32]. For example, users may abandon digital applications if the authentication process is very complex; however, they may abandon faster if there are privacy concerns [32]. Therefore, simplicity should not come at the expense of lower functionality, security or credibility; a certain degree of complexity is necessary to signal functionality [33]. In the same vein, research shows that additional features of a service or product are pleasant for users up to a certain extent, and beyond that, extra features hamper ease of use [34].

Another feature that can impact users' trust is the *appearance and graphical characteristics* of the service or product. For example, research shows that the interface layout and colours are influential in enhancing users' trust in online banking [35].

The ability for users to tailor online products and services to their needs (i.e., customization and personalization) has also been identified as a factor that may influence users' trust [19], [30]. However, since *personalization* requires collecting personal information from users, it could raise concerns for online privacy and adversely impact users' trust [15].

4.1.2 Security & Privacy

Users expect online services to be safe and secure. A recent survey shows that 78% of Canadians are concerned about their personal information being compromised online [36]. Security threats such as destruction of data, disclosure, fraud, unauthorized access, and abuse can be caused by data breaches and attacks on networks [37]. Therefore, proper *security measures* against damage, attacks, and unauthorized access enhance users' trust and service adoption [38]. Particularly, digital and IT-related technologies can create a feeling of being tracked. In this context, some studies have indicated that perceived privacy protection is more important than any potential benefits provided by new technologies [39].

However, a high degree of security and protection might come at the expense of user experience and create cumbersome processes. A cumbersome authentication process could lead to user abandonment. Therefore, the assurance level in online service, which measures the required level of confidence in a digital transaction [5], should be proportional to the risk level of the transaction [6]. The riskier the transaction, the higher the assurance level should be. A high degree of assurance level requires intensive onboarding and strong authentication processes; if a user is presented with what they see as an unnecessarily high assurance level, it can lead to user rejection of the system. The new biometric measures for authentication such as fingerprint, face recognition, and liveness detection can, at the same time, secure and simplify the process [40].

Security and privacy can also be communicated by certificates and labels from third parties who the users already trust [41], and can help to transfer this trust to new and unknown services [42].

4.1.3 Transparency

Given that adopting new technologies, in general, is associated with uncertainty and risk [43], increasing transparency by providing additional information is a means of building trust [41], particularly for technologies that have not yet been established in the marketplace [44]. Nowadays, most users know that data can be collected and sold to third-party agents [45]. As a result, *transparency* about what data is collected [46], where it comes from [44], which third parties can access the information [46] and what it will be used for [47] can mitigate user concerns and be a compelling factor for user adoption [48]. The process by which an online service makes use of data should also be transparent [44]. For example, in cases when an algorithm is behind collecting data and making decisions, highlighting the fact that no human being is involved in the process can enhance trust [49]. However, it has also been shown that people do not have the same attitude toward the proper level of transparency, and a high degree of transparency may result in complexity and data overload [23].

4.1.4 Control

Prior research on smart products and digital technology adoption shows that increased consumer *control* leads to greater trust [23]. Empowerment builds trust, and a lack of control over personal information can cause a sense of disempowerment for some users. Users tend to worry about the lack of control options [38], and most people like to be in control, particularly concerning personal information [50]. A good approach to reducing the initial concern and enhancing trust in new technologies is to initially provide a range of control options, which can gradually be reduced as trust is built [51], [52]. The other factor identified to reduce the mistrust associated with a lack of control is to ask for approval for important decisions [53]. Asking for user approval would protect users against a decision perceived as wrong and make them more confident to use the technology [54].

One important benefit offered by digital ID systems is the user's ability to determine who holds their information, where it's held, and how long it's held for. Users can also update their information, and revoke their previous consent to sharing or exposing their information [6]. These features of digital identity systems play an important role in enhancing users' acceptance and trust.

4.2 Institutional Factors

4.2.1 Brand

The *reputation of a technology provider* or brand serves as another important enabler of trust. Brand, as Batra et al. [55] define reputation as consumers' feelings and perceptions about an item, including its identity, quality, familiarity, and trust identified by a brand name. A well-known brand is a valuable asset that is established over time and has a positive impact on consumers' attitudes toward the quality and performance of a product [56]. Although there is uncertainty associated with any new technology, research shows that users can transfer reputation and reliability for a particular brand to new solutions provided under that brand [57]. In other words, the previously established beliefs about the reliability, safety, and honesty of a brand build trust in a new technology offered by the brand [58].

For example, financial institutions (FIs) are typically trusted by consumers and have already developed a relationship of trust with customers [6]. Thus, users are more likely to trust a digital ID system developed by FIs. A recent survey shows that 81% of Canadians trust financial institutions to keep their personal information safe and secure [36]. Research also shows that the *size* of an online service provider also influences users' view of the trustworthiness of that provider, where larger organizations appear to be more trustworthy [59].

4.2.2 Third-Party Guarantees

Unknown technology providers can use a *third-party guarantee* to boost users' trust in their products or services [60], [61]. Research shows that establishing a link between a trustworthy entity (i.e., a third party) and an unknown one (i.e., a service provider that the third party recommends or confirms) can help in the formation of trust through a transfer process [60]. *Certifications* from trustworthy third parties are effective in promoting users' trust in new technologies [62], especially for assuring the privacy and security policies of e-commerce [63]. A recent study shows that 70% of Canadians feel that the best approach to creating a digital ID is a collaboration between the government and the private sector, and only 16% think that the private sector should take the lead alone [36].

4.2.3 Information & Support

Since the diffusion process of new technologies is characterized by risk and uncertainty [43], *information and support* about a product and its usage, training, and proactively supporting users is a significant factor in building trust [64]. Onboarding users is more important for technologies that are perceived as more complex. If users are not able to easily use the product or service, they feel that they do not have any control over the product, and this lack of control, as mentioned before, is a driver of mistrust [65]. Particularly for technologies that deal with sensitive personal data, informing users about protective measures and security options can significantly enhance users' trust [66]. For example, the quality of information on e-health services was found to be a crucial factor in the development of users' trust [67], [68]. In some research, *lack of awareness of the benefits* of using e-government services was identified as an important barrier to adoption.

4.2.4 Regulation & Standards

Structural assurances such as *regulations and standards* enable individuals and other entities to anticipate a successful future for new technologies and increase their rate of adoption, particularly in the case of technologies such as digital ID, which deals with users' privacy. Regulations and standards also guarantee the existence of other trust enablers. For example, a request for more transparency is among the drivers for the new EU General Data Protection Regulation (GDPR), which came into force in 2018 (Wachter 2018). In the case of digital identity systems, in order to have a viable and sustainable service, both the public and private sector should play a role in developing operational standards that determine regulatory issues such as liability and dispute resolution, business model, and levels of assurance [6].

4.3 Personal Factors

The third category of factors that influence individuals' trust in online technologies is personal factors. Individuals differ in the degree to which they trust their exchange parties [14]. In the context of online exchanges, some users tend to trust anything and anyone and are more likely to use online technologies [69]. Demographic variables, psychological aspects, social interaction, knowledge and experience are determinant factors in the way individuals think about and use technology [39], [70], [71].

4.3.1 Experience

One individual characteristic that helps users to cope themselves in new and unknown environments is *user experience and knowledge*. Users who have experience in dealing with known technologies are more likely to trust new technologies [39]. Corbitt et al. [72], for instance, demonstrate that users' level of internet experience influences their tendency to trust and use online technologies. However, further research shows that the impact of Internet experience on online trust is favourable for new and intermediate users [73]. At higher levels of experience, where users become more knowledgeable about possible online risks, they become more cautious about their privacy and security [74].

4.3.2 Innovativeness

Another individual characteristic is *innovativeness,* which is a personal trait that reflects confidence or optimism regarding the acceptance of new ideas or technologies [75]. Research shows a positive correlation between innovativeness and positive attitudes toward new technologies [76]. Innovative people have an intrinsic interest in trying new technologies, believe in the functionality and reliability of a new product or service, and are some of the first adopters of new technologies [77].

4.3.3 Self-Efficacy

According to the literature, self-efficacy referred to a person's perceived ability to use a technological innovative product [78]. Self-efficacy is an essential motivational variable that influences individuals' intention and effort to use technology, and people with low self-efficacy feel less capable of handling a situation as they feel inadequacy or discomfort [79]. Research shows that people with a high level of self-efficacy are more willing to adopt technology such as online banking and e-government services [52], [80]-[82].

4.3.4 Perceived Risk

Given that the need for trust arises only in situations that involve risk [14], risk tolerance is another factor in assessing the likelihood of adoption. For example, research found that people who value excitement more than security (i.e., excitement-minded vs. security-minded users) tend to perceive more risk regarding e-commerce [83]. These personal values may be endogenous or developed over time and could vary depending on the context and nature of the e-commerce service [7]. For example, Metzger [84] attributes the users' *perceived risk* to their experience with online commerce; people who have more experience with the Internet and e-commerce tend to perceive less risk in online technologies. Research also shows that perceptions of online risk vary according to the sensitivity of personal data used in an online transaction [85]. For example, users are reluctant to disclose not only their confidential personal data such as income, and health-related information, but also their publicly-accessible contact data such as name, postal address, phone number and email [85]. Demographic information such as age and gender are not considered to be very sensitive, but this may not be the case for data such as religion and ethnic background [85]. According to a recent DIACC report [36], Canadians are more comfortable sharing information about their gender, nationality, marital status, and occupation compared to information about their name, income, email, or home address.

4.3.5 Convenience

Users' attitudes toward convenience can influence trust in technology [39]. Research shows that 68% of Canadians are willing to share personal information if it makes their online experience more convenient [36]. Users who are *convenience-oriented* tend to judge convenience as more important than confidence or trust [86]. These people may be more likely to prefer easy-to-use but less-secure technologies compared to more complicated but safer ones.

4.3.6 Uniqueness & Prestige Effect

Views on social interactions can also affect technology adoption. For example, some people tend to desire exclusive products or services that signal their uniqueness and set them apart from their social environment [87], [88]. Similarly, people may choose to own an innovative product as a signal of their prestige [89]-[91]. Since innovative technologies are often associated with *uniqueness* and *prestige*, people with a personal desire for differentiation tend to have a higher willingness to use these technologies [39].

4.3.7 Demographic Variables

Demographic variables such as age, sex, income, education also influence users' disposition of trust. However, these characteristics often mediate the effect of other personal features. For example, older people are found to perceive more risk than younger ones [92]. In the same vein, Liebermann and Stashevsky [93] showed that age, sex, marital status and education impact the perception of risk. According to their research, married people, women, the elderly, and those with low education levels perceive higher risk on the Internet [93].

5 Conclusion

With the rapid and ever-increasing movement of all services to the online and digital realm over the last few years, we need a digital identity system that is highly secure, available everywhere and convenient. However, digital identity relies heavily on trust to succeed, and users must widely adopt the system for society to unlock its benefits. In this review, we have tried to identify all possible building blocks of trust that will be needed for digital identity to succeed.

We've broken down the antecedents of trust in digital services and products into three types of factors: technological, institutional and personal. This review paves the way for a systematic study to measure consumer trust in emerging digital identity services, and to anticipate who the early adopters of these systems will be.

References

[1] 2019.

[2] 2020.

[3] 2018.

[4] 2019.

[5] 2020.

[6] 2016.

[7] D. H. McKnight and N. L. Chervany, "What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology," *International Journal of Electronic Commerce,* vol. 6, *(2),* pp. 35-59, 2001.

[8] T. K. Das and B. Teng, "The risk-based view of trust: A conceptual framework," *Journal of Business and Psychology,* vol. 19, *(1),* pp. 85-116, 2004.

[9] J. B. Rotter, "A new scale for the measurement of interpersonal trust 1," *J. Pers.,* vol. 35, *(4),* pp. 651-665, 1967.

[10] J. G. Holmes, "Trust and the appraisal process in close relationships." 1991.

[11] A. Bauman and R. Bachmann, "Online consumer trust: Trends in research," *Journal of Technology Management & Innovation,* vol. 12, *(2),* pp. 68-79, 2017.

[12] G. Dietz, "Going back to the source: Why do people trust each other?" *Journal of Trust Research,* vol. 1, *(2),* pp. 215-222, 2011.

[13] R. Botsman, Who can You Trust?: How Technology Brought Us Together and Why it might Drive Us Apart. 2017.

[14] R. C. Mayer, J. H. Davis and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review,* vol. 20, *(3),* pp. 709-734, 1995.

[15] A. Beldad, M. De Jong and M. Steehouder, "How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust," *Comput. Hum. Behav.,* vol. 26, *(5),* pp. 857-869, 2010.

[16] C. L. Corritore, B. Kracher and S. Wiedenbeck, "On-line trust: concepts, evolving themes, a model," *International Journal of Human-Computer Studies,* vol. 58, *(6),* pp. 737-758, 2003.

[17] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly,* pp. 319-340, 1989.

[18] F. D. Davis, "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts," *International Journal of Man-Machine Studies,* vol. 38, *(3),* pp. 475-487, 1993.

[19] A. Adjekum, A. Blasimme and E. Vayena, "Elements of trust in digital health systems: scoping review," *Journal of Medical Internet Research,* vol. 20, *(12),* pp. e11254, 2018.

[20] B. H. Wixom and P. A. Todd, "A theoretical integration of user satisfaction and technology acceptance," *Information Systems Research,* vol. 16, *(1),* pp. 85-102, 2005.

[21] C. Wilson, T. Hargreaves and R. Hauxwell-Baldwin, "Benefits and risks of smart home technologies," *Energy Policy,* vol. 103, pp. 72-83, 2017.

[22] B. F. Yuksel, P. Collisson and M. Czerwinski, "Brains or beauty: How to engender trust in user-agent interactions," *ACM Transactions on Internet Technology (TOIT),* vol. 17, *(1),* pp. 1-20, 2017.

[23] D. S. Johnson, F. Bardhi and D. T. Dunn, "Understanding how technology paradoxes affect customer satisfaction with self-service technology: The role of performance ambiguity and trust in technology," *Psychology & Marketing,* vol. 25, *(5),* pp. 416-443, 2008.

[24] M. Pagani, "Determinants of adoption of third generation mobile multimedia services," *Journal of Interactive Marketing,* vol. 18, *(3),* pp. 46-59, 2004.

[25] B. J. Dietvorst, J. P. Simmons and C. Massey, "Algorithm aversion: People erroneously avoid algorithms after seeing them err." *J. Exp. Psychol. : Gen.,* vol. 144, *(1),* pp. 114, 2015.

[26] N. P. Rana *et al*, "Theories and theoretical models for examining the adoption of e-government services," *E-Service Journal: A Journal of Electronic Services in the Public and Private Sectors,* vol. 8, *(2),* pp. 26-56, 2012.

[27] C. Flavián, M. Guinalíu and R. Gurrea, "The role played by perceived usability, satisfaction and consumer trust on website loyalty," *Information & Management,* vol. 43, *(1),* pp. 1-14, 2006.

[28] Y. Bart *et al*, "Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study," *J. Market.,* vol. 69, *(4),* pp. 133-152, 2005.

[29] C. Chen, "Identifying significant factors influencing consumer trust in an online travel site," *Information Technology & Tourism,* vol. 8, *(3-4),* pp. 197-214, 2006.

[30] M. Koufaris and W. Hampton-Sosa, "The development of initial trust in an online company by new customers," *Information & Management,* vol. 41, *(3),* pp. 377-397, 2004.

[31] D. Gefen, E. Karahanna and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quarterly,* vol. 27, *(1),* pp. 51-90, 2003.

[32] 2018.

[33] E. Eytam, N. Tractinsky and O. Lowengart, "The paradox of simplicity: Effects of role on the preference and choice of product visual simplicity level," *International Journal of Human-Computer Studies,* vol. 105, pp. 43-55, 2017.

[34] S. A. Rijsdijk and E. J. Hultink, "How today's consumers perceive tomorrow's smart products," *J. Prod. Innovation Manage.,* vol. 26, *(1),* pp. 24-42, 2009.

[35] J. Kim and J. Y. Moon, "Designing towards emotional usability in customer interfaces—trustworthiness of cyber-banking system interfaces," *Interact Comput,* vol. 10, *(1),* pp. 1-29, 1998.

[36] August. 2019.

[37] F. Belanger, J. S. Hiller and W. J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems,* vol. 11, *(3-4),* pp. 245-270, 2002.

[38] V. Kumar *et al*, "Research framework, strategies, and applications of intelligent agent technologies (IATs) in marketing," *Journal of the Academy of Marketing Science,* vol. 44, *(1),* pp. 24-45, 2016.

[39] K. Wiedmann *et al*, "Determinants of consumers' perceived trust in IT-ecosystems," *Journal of Theoretical and Applied Electronic Commerce Research,* vol. 5, *(2),* pp. 137-154, 2010.

[40] A. Goode, "Digital identity: solving the problem of trust," *Biometric Technology Today,* vol. 2019, *(10),* pp. 5-8, 2019.

[41] M. Wißner *et al*, "Trust-based decision-making for the adaptation of public displays in changing social contexts," *Journal of Trust Management,* vol. 1, *(1),* pp. 6, 2014.

[42] K. C. Lee, I. Kang and D. H. McKnight, "Transfer from offline trust to key online perceptions: an empirical study," *IEEE Trans. Eng. Manage.,* vol. 54, *(4),* pp. 729-741, 2007.

[43] E. M. Rogers, Diffusion of Innovations. 2010.

[44] A. Glass, D. L. McGuinness and M. Wolverton, "Toward establishing trust in adaptive agents," in *Proceedings of the 13th International Conference on Intelligent User Interfaces,* 2008, .

[45] K. L. Walker, "Surrendering information through the looking glass: Transparency, trust, and protection," *Journal of Public Policy & Marketing,* vol. 35, *(1),* pp. 144-158, 2016.

[46] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly,* pp. 13-28, 2006.

[47] J. Lahtiranta, S. Hyrynsalmi and J. Koskinen, "The false prometheus: customer choice, smart devices, and trust," *ACM SIGCAS Computers and Society,* vol. 47, *(3),* pp. 86-97, 2017.

[48] H. Treiblmaier and I. Pollach, "Users' perceptions of benefits and costs of personalization," *ICIS 2007 Proceedings,* pp. 141, 2007.

[49] (). *Who Made That Decision: You or an Algorithm?*. Available: https://knowledge.wharton.upenn.edu/article/algorithms-decision-making/.

[50] J. Phelps, G. Nowak and E. Ferrell, "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing,* vol. 19, *(1),* pp. 27-41, 2000.

[51] M. Child and N. Linketscher, "Trust issues and user reactions to e-services and electronic marketplaces: a customer survey," *Hp Laboratories Technical Report Hpl, (32),* 2001.

[52] Z. Mani and I. Chouk, "Drivers of consumers' resistance to smart products," *Journal of Marketing Management,* vol. 33, *(1-2),* pp. 76-97, 2017.

[53] E. Heiskanen *et al*, "User involvement in radical innovation: are consumers conservative?" *European Journal of Innovation Management,* 2007.

[54] D. J. Cook, J. C. Augusto and V. R. Jakkula, "Ambient intelligence: Technologies, applications, and opportunities," *Pervasive and Mobile Computing,* vol. 5, *(4),* pp. 277-298, 2009.

[55] R. Batra, A. Ahuvia and R. P. Bagozzi, "Brand love," *J. Market.,* vol. 76, *(2),* pp. 1-16, 2012.

[56] A. B. Del Rio, R. Vazquez and V. Iglesias, "The effects of brand associations on consumer response," *Journal of Consumer Marketing,* 2001.

[57] C. Zehir *et al*, "The effects of brand communication and service quality in building brand loyalty through brand trust; the empirical research on global brands," *Procedia-Social and Behavioral Sciences,* vol. 24, pp. 1218-1231, 2011.

[58] E. Delgado-Ballester and J. L. Munuera-Alemán, "Brand trust in the context of consumer loyalty," *European Journal of Marketing,* 2001.

[59] S. L. Jarvenpaa, N. Tractinsky and M. Vitale, "Consumer trust in an Internet store," *Information Technology and Management,* vol. 1, *(1-2),* pp. 45-71, 2000.

[60] P. M. Doney, J. P. Cannon and M. R. Mullen, "Understanding the influence of national culture on the development of trust," *Academy of Management Review,* vol. 23, *(3),* pp. 601-620, 1998.

[61] S. H. Ha and L. T. Liu, "Critical success factors of open markets on the internet in terms of buyers," in *Conference on E-Business, E-Services and E-Society,* 2010, .

[62] D. Koehn, "The nature of and conditions for online trust," *J. Bus. Ethics,* vol. 43, *(1-2),* pp. 3-19, 2003.

[63] C. M. Cheung and M. K. Lee, "Understanding consumer trust in Internet shopping: A multidisciplinary approach," *J. Am. Soc. Inf. Sci. Technol.,* vol. 57, *(4),* pp. 479-492, 2006.

[64] M. Naor *et al*, "Overcoming barriers to adoption of environmentally-friendly innovations through design and strategy," *International Journal of Operations & Production Management,* 2015.

[65] S. A. Rijsdijk and E. J. Hultink, "“Honey, have you seen our hamster?” Consumer evaluations of autonomous domestic products," *J. Prod. Innovation Manage.,* vol. 20, *(3),* pp. 204-216, 2003.

[66] S. Hammer, M. Wißner and E. André, "Trust-based decision-making for smart and adaptive environments," *User Modeling and User-Adapted Interaction,* vol. 25, *(3),* pp. 267-293, 2015.

[67] E. Sillence et al, "Trust and mistrust of online health sites," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2004, .

[68] E. Sillence *et al*, "Health websites that people can trust–the case of hypertension," *Interact Comput,* vol. 19, *(1),* pp. 32-42, 2007.

[69] A. F. Salam *et al*, "Trust in e-commerce," *Commun ACM,* vol. 48, *(2),* pp. 72-77, 2005.

[70] D. Johnson and K. Grayson, "Cognitive and affective trust in service relationships," *Journal of Business Research,* vol. 58, *(4),* pp. 500-507, 2005.

[71] S. Grabner-Kräuter and E. A. Kaluscha, "Empirical research in on-line trust: a review and critical assessment," *International Journal of Human-Computer Studies,* vol. 58, *(6),* pp. 783-812, 2003.

[72] B. J. Corbitt, T. Thanasankit and H. Yi, "Trust and e-commerce: a study of consumer perceptions," *Electronic Commerce Research and Applications,* vol. 2, *(3),* pp. 203-215, 2003.

[73] K. D. Aiken and D. M. Boush, "Trustmarks, objective-source ratings, and implied investments in advertising: investigating online trust and the context-specific nature of internet signals," *Journal of the Academy of Marketing Science,* vol. 34, *(3),* pp. 308-323, 2006.

[74] M. Z. Yao, R. E. Rice and K. Wallis, "Predicting user concerns about online privacy," *J. Am. Soc. Inf. Sci. Technol.,* vol. 58, *(5),* pp. 710-722, 2007.

[75] R. Agarwal and J. Prasad, "A conceptual and operational definition of personal innovativeness in the domain of information technology," *Information Systems Research,* vol. 9, *(2),* pp. 204-215, 1998.

[76] W. M. Lassar, C. Manolis and S. S. Lassar, "The relationship between consumer innovativeness, personal characteristics, and online banking adoption," *International Journal of Bank Marketing,* 2005.

[77] D. H. McKnight, V. Choudhury and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Information Systems Research,* vol. 13, *(3),* pp. 334-359, 2002.

[78] D. R. Compeau and C. A. Higgins, "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly,* pp. 189-211, 1995.

[79] M. E. Gist, C. Schwoerer and B. Rosen, "Effects of alternative training methods on self-efficacy and performance in computer software training." *J. Appl. Psychol.,* vol. 74, *(6),* pp. 884, 1989.

[80] P. Chatzoglou, D. Chatzoudes and S. Symeonidis, "Factors affecting the intention to use e-government services," in *2015 Federated Conference on Computer Science and Information Systems (FedCSIS),* 2015, .

[81] N. P. Rana and Y. K. Dwivedi, "Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT)," *Government Information Quarterly,* vol. 32, *(2),* pp. 172-181, 2015.

[82] W. Nasri and L. Charfeddine, "Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior," *The Journal of High Technology Management Research,* vol. 23, *(1),* pp. 1-14, 2012.

[83] K. Pennanen, T. Tiainen and H. T. Luomala, "A qualitative exploration of a consumer's value-based e-trust building process," *Qualitative Market Research: An International Journal,* 2007.

[84] M. J. Metzger, "Effects of site, vendor, and consumer characteristics on web site trust and disclosure," *Communication Research,* vol. 33, *(3),* pp. 155-179, 2006.

[85] A. Beldad, M. De Jong and M. Steehouder, "I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions," *Comput. Hum. Behav.,* vol. 27, *(6),* pp. 2233-2242, 2011.

[86] S. L. Lokken *et al*, "Comparing online and non-online shoppers," *International Journal of Consumer Studies,* vol. 27, *(2),* pp. 126-133, 2003.

[87] T. M. Verhallen and H. S. Robben, "Scarcity and preference: An experiment on unavailability and product evaluation," *Journal of Economic Psychology,* vol. 15, *(2),* pp. 315-331, 1994.

[88] M. Lynn, "Scarcity effects on value: A quantitative review of the commodity theory literature," *Psychology & Marketing,* vol. 8, *(1),* pp. 43-57, 1991.

[89] R. W. Belk, "Possessions and the extended self," *Journal of Consumer Research,* vol. 15, *(2),* pp. 139-168, 1988.

[90] H. Dittmar, "Material possessions as stereotypes: Material images of different socio-economic groups," *Journal of Economic Psychology,* vol. 15, *(4),* pp. 561-585, 1994.

[91] E. Chang, F. Hussain and T. Dillon, Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence. 2006.

[92] J. E. Grable and S. Joo, "Factors related to risk tolerance: A further examination," *Consumer Interests Annual,* vol. 45, *(1),* pp. 53-58, 1999.

[93] Y. Liebermann and S. Stashevsky, "Perceived risks as barriers to Internet and e-commerce usage," *Qualitative Market Research: An International Journal,* 2002.