Key Factors Affecting User Adoption of Open-Access Data Repositories in Intelligence and Security Informatics: An Affordance Perspective

10

BO WEN and PAUL JEN-HWA HU, Department of Operations and Information Systems, David Eccles School of Business, University of Utah, UT, USA
MOHAMMADREZA EBRAHIMI, School of Information Systems and Management, Muma College of Business, University of South Florida, FL, USA
HSINCHUN CHEN, Department of Management Information Systems, University of Arizona, AZ, USA

Rich, diverse cybersecurity data are critical for efforts by the **intelligence and security informatics (ISI)** community. Although **open-access data repositories (OADRs)** provide tremendous benefits for ISI researchers and practitioners, determinants of their adoption remain understudied. Drawing on affordance theory and extant ISI literature, this study proposes a factor model to explain how the essential and unique affordances of an OADR (i.e., relevance, accessibility, and integration) affect individual professionals' intentions to use and collaborate with AZSecure, a major OADR. A survey study designed to test the model and hypotheses reveals that the effects of affordances on ISI professionals' intentions to use and collaborate are mediated by perceived usefulness and ease of use, which then jointly determine their perceived value. This study advances ISI research by specifying three important affordances of OADRs; it also contributes to extant technology adoption literature by scrutinizing and affirming the interplay of essential user acceptance and value perceptions to explain ISI professionals' adoptions of OADRs.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**;

Additional Key Words and Phrases: Intelligence and security informatics, open-access data repositories, affordance theory, user technology adoption, perceived value, technology acceptance

ACM Reference format:
Bo Wen, Paul Jen-Hwa Hu, Mohammadreza Ebrahimi, and Hsinchun Chen. 2021. Key Factors Affecting User Adoption of Open-Access Data Repositories in Intelligence and Security Informatics: An Affordance Perspective. *ACM Trans. Manage. Inf. Syst.* 13, 1, Article 10 (October 2021), 24 pages.
https://doi.org/10.1145/3460823

This work was partially funded by the National Science Foundation, Data Infrastructure Building Blocks (DIBBs) Program, "CIF21: DIBBs for Intelligent and Security Informatics Research and Community," October 2014 – September 2018, ACI-1443019.

Authors' addresses: B. Wen and P. J.-H. Hu, Department of Operations and Information Systems, David Eccles School of Business, University of Utah, UT, USA; M. Ebrahimi, School of Information Systems and Management, Muma College of Business, University of South Florida, FL, USA; H. Chen, Department of Management Information Systems, University of Arizona, AZ, USA.

2158-656X/2021/10-ART10 $15.00
https://doi.org/10.1145/3460823

1 INTRODUCTION

Cybersecurity entails the processes or capabilities to protect **information systems (IS)** against damage and unauthorized use.[1] Common threats include hacking (e.g., ransomware) [17], stolen financial information [14], malicious source code [7], and insider threats [10], each of which can impose enormous damages on individuals and organizations. The cost of cyberattacks has increased from US$11.7 million per company in 2017 to US$13 million by 2019 [9]. To reduce damages, cybersecurity relies on **intelligence and security informatics (ISI)** for insights into cyber threats (risks) and developments of effective safeguards and countermeasures [11].

To be effective, ISI needs convenient access to relevant data from different sources, which facilitates knowledge reproducibility and discoverability [39]. Yet such data are difficult to obtain, due to various technical, organizational, and social constraints [47]. To illustrate, online hacker forums often implement barriers, such as requiring registered user accounts, imposing session timeouts to restrict server connection time, installing cookies to track individual behaviors, and requiring periodic entries of some combination of hard-to-recognize alphanumeric characters to prevent automated crawling programs from accessing the platforms [14]. **Open-access data repositories (OADRs)** can provide a solution, because they contain rich, diverse data from various sources and are publicly available in a single location. Considering the potential benefits of such repositories, we examine ISI professionals' decisions to use and collaborate with AZSecure, an OADR that offers large-scale data sets for cybersecurity research.[2] It maintains tens of millions of entries (records) pertaining to the dark net, social media content, malware binaries, and network traffic logs.[3] Using affordance theory [20], we identify key factors affecting ISI professionals' adoptions of AZSecure, through the influences of perceived usefulness, ease of use, and value.

2 LITERATURE REVIEW

2.1 ISI Research and Data Requirements

As summarized in Table 1, existing ISI research [7, 46] identifies integration, access, and relevance as three crucial data requirements for cybersecurity that aims to reduce the harms of fake websites [1], the dark net [16], and hacker communities [46]. First, integration involves data from different sources. Abbasi et al. [1] integrated an enormous number of media news articles as well as reports by the National Association of Boards of Pharmacy to detect fraudulent medical websites created by cybercriminals. Second, access refers to processes or tools for capturing data without restrictions. For example, by using tor-routed browsers, researchers can anonymously access dark net marketplaces by circumventing their anti-crawling measures [16]. Several studies focus on hacker communities, using specialized tools to collect hacker forum data [7, 46, 57]. Third, the collected data need to be relevant to the objective of an ISI professional's analysis. Relevant contents in the dark net might include forum postings, author names, and thread titles, which can be extracted by advanced parser programs [7]. These efforts usually require specialized procedures, such as Samtani et al.'s [46] method to extract source code, attachments, or tutorial posts on the basis of special HTML tags generated in hacker forums. According to our literature review and in-depth interviews with eight voluntary ISI professionals, we identify three essential data requirements: (1) multiple data sources [1–3, 33, 40, 57], (2) specialized tools or processes to access vast amounts

[1] https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C, accessed on October 26, 2020.

[2] AZSecure, an open-access data repository for the ISI community, is created and maintained through a joint effort by five universities, as part of an NSF-funded project; see https://www.AZSecure-data.org/ for details.

[3] The dark web incorporates a conglomerate of illegal platforms (e.g., hacker forums, chat rooms, dark net marketplaces) across the surface and deep web, which facilitates exchanges and communications among cybercriminals. Dark net markets, as part of the dark web that are not accessible by search engines on the surface web, host illegal anonymous platforms [16].

Table 1. Representative ISI Studies and Associated Data Requirements

Study	Focal Domain	Use of Multiple Data Sources	Tool or Process for Information Access	Relevant Information Extracted
Abbasi et al. [1]	Fake websites	Yes: National Association of Boards of Pharmacy, Medical Library Association's consumer, LegitScript, and others	Direct downward	Legitimate and fake medical websites
Abbasi et al. [2]	Fake websites	Yes: Phishtank.com and Anti-Phishing Working Group	Automated spidering program	Legitimate, concocted, spoof sites
Abbasi et al. [3]	Fake websites	Yes: Phishtank.com and Anti-Phishing Working Group	Automated spidering program	Legitimate, concocted and spoof websites
Benjamin et al. [7]	Dark net	Yes: Multiple underground Web communities	Automatic web crawler	Forum postings, author names, thread titles
Benjamin et al. [8]	Hacker communities	Yes: Two large IRC channels	IRC listener	Tor network messages
Du et la. [14]	Hacker communities	Yes: Hacker forums, IRC, dark net market, carding shops	Tor-routed web crawler and IRC bots	Posts, conversations, listings
Ebrahimi et al. [16]	Dark net	Yes: 9 Dark net marketplaces	Tor-routed web crawler	Product listings
Li et al. [33]	Hacker communities	Yes: 8 forum-based underground economies	Thread crawler	Customer reviews, seller characteristics
Pierazzi et al. [40]	Hacker communities	No: VirusTotal	Virus Total API	Spyware, goodware, malware samples from Virus Total
Qin et al. [43]	Dark net	Yes: Government reports, research centers, and search engines	Automatic web crawler	HTML elements, embedded multimedia, hyperlink, email list, etc.
Samtani et al. [46]	Hacker communities	Yes: 7 hacker forums	Tor-routed web crawler	Source code, attachment, tutorial posts
Yue et al. [57]	Hacker communities	Yes: One hacker forum, network logs, and two vulnerability databases	Direct download	DDOS-attack posts

of data [7, 32, 43, 57], and (3) relevant data with respect to the intended ISI analyses [7, 8, 14, 16, 46].

2.2 User Adoption of Open-Access Data Repositories

Open-access data repositories can meet these essential data requirements. The development and maintenance of an OADR require substantial time, effort, and monetary resources; yet its value can be realized only if individuals adopt and use it in their work. We define an OADR as a set of systems and services that allow users to inspect, access, and integrate relevant data from different sources

with minimal restrictions [41].[4] Broadly, OADRs have two objectives. First, an OADR ensures data provisions by making data publicly available to targeted users, which reflects a user-centric orientation with a focus on individual intentions to use the OADR [56, 60]. Second, an OADR fosters collaboration among users, which is also critical to their use of the OADR [30]. Accordingly, we examine ISI professionals' intentions to use OADRs and collaborate in that use.

However, previous OADR adoption research seldom considers the unique ISI domain. Many studies tend to focus on perceived value or user acceptance perspectives exclusively (see Table 2). People perceive benefits and barriers to use, which are crucial precursors to their adoption decisions. In reviewing government agencies' adoption of OADRs, Janssen et al. [33] report a strong effect of value perceptions on the basis of benefit versus barrier assessments. Perceived benefits (e.g., transparency, accountability) also emerge as essential motivators for public users' OADR adoptions [4]. A case study [28] shows an association of perceived value (e.g., promoting civic management) and intention to use an OADR, a link that also has been observed in quantitative studies, such as Wang and Lo's [55] survey of government agencies' adoptions of OADRs as well as Weerakkody et al.'s [56] test of the effects of values on individuals' intentions to use OADRs.

Alternatively, another perspective prioritizes user acceptance, as exemplified in a study relying on the **technology acceptance model (TAM)** to show that perceived ease of use and usefulness affect individual intentions to use OADRs [44]. Dulle and Minishi-Majanja [15] use the unified theory of acceptance and use of technology model to predict researchers' acceptance of OADRs. Zuiderwijk et al. [60] report that users' performance and effort expectancy influence their decisions to use OADRs provided by government institutions. These studies emphasize user acceptance and indicate that key user perceptions (e.g., usefulness, ease of use) affect acceptance.

2.3 AZSecure

AZSecure is a major OADR that provides various large-scale cybersecurity data sets to the ISI community [48]. As shown in Figure 1, it contains millions of security entries (records), extracted from the dark net, fake websites, social media (e.g., Twitter), malware repositories, and network traffic logs. Textual data are available in different languages (e.g., English, Russian, Chinese, French, German). AZSecure consists of data infrastructure building blocks to make relevant data conveniently accessible to targeted users. As a partially funded project by the National Science Foundation, all data sets in AZSecure can be downloaded for non-commercial education and research use, free of charge. AZSecure's rich marketplace data contain hundreds of thousands of illegal products advertised on the dark net along with vendor information. These data include product description, price, shipping information, and seller information. AZSecure's hacker forum data feature millions of posts, detailed by content, topic, and posting date, as well as information about their authors (e.g., screen name, reputation). The IRC data encompass messages by anonymous hackers and hacktivist groups. The fake website data feature thousands of phishing websites and web addresses created by cybercriminals to launch fraudulent banking transactions or steal financial account information. The Twitter contents include tweets about security topics (e.g., anti-virus). The malware data contain real malware binaries collected from multiple sources (e.g., honeypots, mail filters, proxy monitors, file sharing networks). Finally, the network traffic data encompass flows and logs collected from mid-sized computer networks.

With its rich and diverse contents, AZSecure can support a broad range of ISI analysis tasks, including proactive cyber threat intelligence, cybercriminal network analyses, hacker asset

[4]Although related to open-access data repositories, an open-access article repository usually focuses on academic articles rather than data sets and aims at facilitating article contributions and sharing by individuals or institutions; thus, such repositories are outside the scope of this study.

Table 2. Representative Studies of Open-Access Data Repositories

Study	Content	Method	Consideration of User Acceptance	Consideration of Perceived Value	Dependent Variable(s)
Fry et al. [18]	Journal articles	Survey	No	No	Researchers' use of OADRs across disciplines
Dulle and Minishi-Majanja [5]	Scholarly articles	Survey	Yes, performance and effort expectance	No	Researchers' intention to use OADRs
Kistler et al. [30]	Biomedical data	Design and use cases	No	Yes, value for research collaboration	Designing an OADR and describing researchers' adoption with use cases
Altayar [4]	Government data	Interview	No	Yes, perceived benefits (e.g., transparency, accountability)	Intention to use OADRs by general public
Janssen et al. [26]	Public data	Interview	No	Yes, political, social, economic, operational and technical benefits versus barriers (values)	Intention to use OADRs by data provider
Kassen [28]	Government data	Case study	No	Yes, value for promoting civic engagement	Intention to use OADRs by general public
Fitriani et al. [44]	Public data	Survey	Yes, perceived ease of use and usefulness	No	Intention to continue using OADRs by general public
Wang and Lo [55]	Government data	Survey	No	Yes, perceived benefits and barriers	Government agencies' intentions to use OADRs
Zuiderwijk et al. [60]	Government data	Survey	Yes, performance and effort expectance	No	Intention to use OADRs by general public
Weerakkody et al. [56]	Public data	Survey	No	Functional values, such as relative advantage and complexity	Intention to use OADRs by general public
This study	Cybersecurity data	Survey	Yes, perceived ease of use and usefulness	Yes, perceived value (quality, emotional, social, and economic value)	ISI professionals' intentions to use an OADR and collaborate with it

detections, social media analytics, static and dynamic malware analyses, and network intrusion detection system designs. It has drawn growing attention from researchers and practitioners worldwide, who downloaded 3.0 terabytes of data in 24,939 file requests between July 2018 and September 2019. Many studies facilitated by AZSecure have appeared in leading IS journals and ISI conferences (e.g., *Journal of Management Information Systems, IEEE Intelligent Systems, IEEE Intelligence and Security Informatics Conference*, and *IEEE International Conference on Data Mining*).[5] Yet,

[5]While alternative OADRs are available in IS, they often are out of date and their data contents seem application-specific (e.g., networking, dark net market). Instead, AZSecure is an up-to-date, multi-source repository that contains rich, diverse data pertinent to different ISI areas, such as dark web analytics, hacker forums, and IRC analytics.

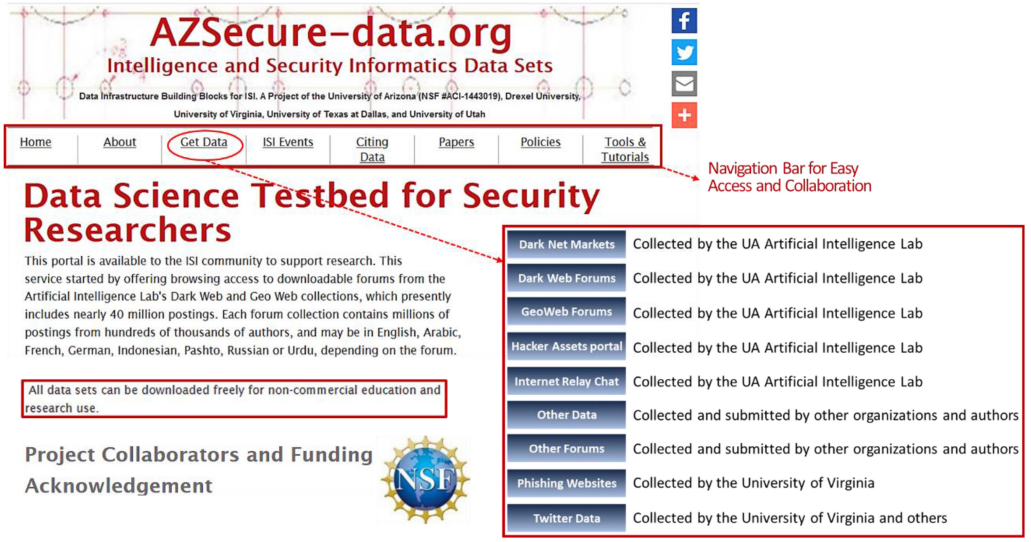


Fig. 1. Snapshots of AZSecure overview and representative data set.

insights into the key factors that affect ISI professionals' adoptions of AZSecure are lacking, though such insights can further improve AZSecure in both design and utilization.

2.4 Gap Analysis

As derived from Table 2, we identify three important research gaps. First, few studies analyze and empirically examine the adoption of OADRs by ISI researchers and practitioners. Previous studies investigate different contexts but lack appropriate considerations of context-specific factors. By leveraging the essential data requirements of the ISI community (Table 1), we stress that three affordances are crucial to targeted users' adoptions of an OADR: accessibility, relevance, and integration. Users must believe that an OADR (e.g., AZSecure) grants them easy access to data [38]. Because accessing valuable cybersecurity data in cyberspace often requires specialized tools or processes to evade anti-crawling measures, the effortless and convenient access to rich data should be a critical benefit that users seek from an OADR [46]. Also, users need to conceive that the OADR provides data relevant to their tasks [38]. Not all data captured in cyberspace are actually useful; in effect, ISI professionals often struggle with retrieving (extracting) adequate data (e.g., product listings, author names) for their analysis tasks [7, 16, 57]. Additionally, users should perceive that an OADR enables them to easily integrate data from various sources [38], such that they can perform complex, broad, and challenging cybersecurity analyses. Second, most previous research primarily focuses on either a user acceptance or a perceived value perspective; instead, we conjecture that using them as complements can provide more accurate predictions of ISI professionals' adoptions of OADRs. Conceivably, people would not adopt a technology artifact if they anticipate it offers less value, regardless of its ease of use or usefulness [29, 52]. A model that incorporates both perspectives can depict the user adoption decision more holistically. Third, empirical examinations of individual intentions to use an OADR to collaborate have received little attention (see Table 2). Collaborations are crucial for the ISI community and can be supported by OADRs. To address these gaps, we propose a factor model to explain ISI professionals' intentions to use AZSecure and collaborate with it by integrating both user acceptance and perceived value perspectives. Particularly, our model includes important factors unique to the ISI context (e.g., essential affordances).

3 THEORETICAL FOUNDATION

We use affordance theory [20], which has attracted growing attention in IS research [50, 58], as a foundation to develop our research model. This theory proposes that people's decisions to use an object are shaped by their perceived affordances of that object. As Gibson [21] defines it, affordance is "what it (an object) offers (to people), what it provides or furnishes" (p. 139). We thus specify affordances as features that a technology artifact offers to users. Affordances are not determined by the object's properties or user characteristics; rather, they reflect the interplay between them [42]. For instance, the visibility of work processes is an essential affordance for individuals' use of dashboards in an organization to manage its business processes [58]. As another example, data capturing is a crucial affordance for healthcare personnel's setting up databases to support patient data access [50]. Because affordances are context dependent and reflect diverse technologies and users, it is crucial to analyze the important affordances unique to the focal context.

Affordances steer individuals' use of an object via a three-stage process: existence, perception, and actualization [42]. Existence reflects a cognitive process, through which people become aware of what an object can afford them (e.g., convenient access to integrated data in a single location). Then perception is a recognition process, such that people check for the essential affordance, using internal evaluations (e.g., usefulness, ease of use) that indicate the value or benefits associated with the affordance. Finally, actualization is "actions taken by actors" to realize the perceived value, "as they take advantage of one or more affordances through their use of the technology" [50] (p. 70). This three-stage process also underscores the mechanisms leading to user adoption.

In our context, affordance existence entails the identification of the three affordances provided by an OADR: integration, accessibility, and relevance. Affordance actualization involves ISI professionals' usage and collaboration intentions, according to their value perceptions. However, it is difficult to identify the affordance perception stage, so we theorize about it by incorporating core constructs from the TAM (i.e., perceived usefulness and ease of use) with the concept of perceived value, to augment our use of affordance theory. Specifically, we predict that affordance perceptions in our study context involve a person's utilitarian evaluation of the affordances of the OADR, followed by the value assessment. Thus, perceived usefulness and ease of use might serve as mediators to link affordances with perceived value, which then leads to affordance actualization.

We rely on these two core constructs from the TAM, because they encapsulate individual evaluations of the affordances of a focal object, without involving other, extended considerations (e.g., social or economic value) [52]. As Davis [13] explains, perceived usefulness is "the degree to which a person believes that using a particular system would enhance his or her job performance," and perceived ease of use is "the degree to which a person believes that using a particular system would be free of effort" (p. 320). Both assessments pertain to individuals' evaluations of what a technology artifact can provide to them at a higher and more abstract level (e.g., effortless, performance enhancement) [54]. Meanwhile, awareness of different affordances and specific features that the artifact provides at a more granular level likely occurs prior to these perceptions.

A person's adoption of a technology artifact also should involve his or her perception of its value, which Zeithaml [59] describes as a person's "overall assessment of the utility of a product (or service) based on perceptions of what is received and what is given" (p. 14). Such value assessments can be influenced by perceived usefulness and ease of use. Perceived usefulness indicates outcome expectancy, which helps users appraise what they would "receive" by using a technology. On the other hand, perceived ease of use reflects a process expectancy, which is central to evaluations of what they need to "give" in order to use the technology [54]. Whereas perceived usefulness and ease of use refer to expectancies pertaining to the performance (outcome) and effort (process) associated with technology uses [6], perceived value depends on benefit–cost trade-offs,

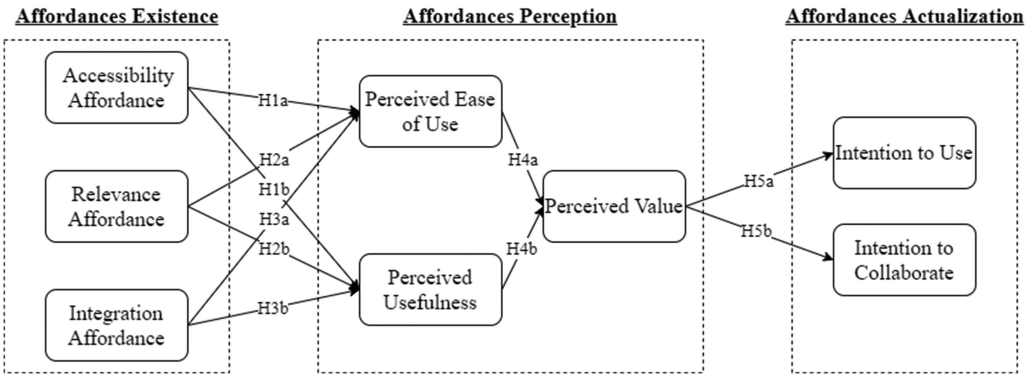


Fig. 2. Research model.

measured by time requirements, monetary costs, cognitive effort, emotional burdens, or social needs [52]. Hence, only assessing perceived usefulness and ease of use may not reflect adoption decisions fully. People who previously have purchased cybersecurity data might deem OADRs a low-cost alternative, so only considering essential user acceptance perceptions would not capture the (economic) value of OADRs. We therefore predict that ISI professionals' decisions to adopt an OADR are shaped by their value assessments [60] and data content quality [26]. Previous research concurs with our prediction that perceived value can explain user adoption of OADRs [26, 55], though without addressing the ISI context. From the lens of affordance theory, we seek to clarify how potential users' value perceptions of an OADR influence their adoption decisions, according to their assessments of the provided utilities.

4 RESEARCH MODEL AND HYPOTHESES

In our research model (Figure 2), affordances affect people's perceptions of AZSecure's usefulness and ease of use, which influence their value evaluations and determine their adoption decisions.

Convenient data access with minimal efforts is a critical affordance that AZSecure offers users, which should affect their perceived ease of use or effort expectancy, because greater accessibility gives users easy access with less frustration [12]. Cybersecurity data are difficult to access [16], so AZSecure can enhance individuals' ease-of-use perceptions. Affording access to data in a single location also may help users sense greater usefulness. The design of AZSecure actively avoids "siloed metadata" that can prevent users from accessing contents "without adequate prior knowledge" [48]. Accessibility affordance, due to these adequate navigation design elements, should enhance perceived usefulness too, because AZSecure helps users locate data and contents efficiently. Therefore, we hypothesize:

H1: Accessibility affordance of AZSecure relates positively to its (a) ease of use and (b) usefulness, as perceived by users.

Relevance affordance means individuals can readily obtain relevant data, which should be positively associated with perceived ease of use. Prior ISI research [7, 46] highlights the importance of specialized knowledge and structures that help users extract only those pieces of information relevant to their needs (e.g., thread title, number of likes, post content). AZSecure provides detailed descriptions of each data set's content (e.g., attribute fields, date ranges) to facilitate data retrievals and extractions. Perceived ease of use thus should be enhanced by users' ability to retrieve relevant data efficiently and effectively from AZSecure, "to support their desired analytical goals" [48]

(p. 2). Additionally, relevance also implies a link with outcome expectancy; i.e., perceived usefulness. The design of AZSecure targets relevance affordance and provides ample information, including a "ReadMe" file describing the data collection, data format, and recommended analytics methods. Such forms of relevance affordance are useful for ISI professionals who can apply similar methods to their own data collections or seek knowledge replication and validation. We thus hypothesize:

H2: Relevance affordance of AZSecure is positively related to its (a) ease of use and (b) usefulness, as perceived by users.

Integration affordance relates to perceived ease of use positively, because combining data from different sources often demands substantial time and effort [1, 33]. The design of AZSecure aims at serving as a one-stop repository that meets ISI professionals' data needs for comprehensive analyses of various cybersecurity issues. Thus, researchers and practitioners can save time that they otherwise would have devoted to data integrations, and allocate that effort to analyses instead. Integration affordance contributes to the usefulness of AZSecure too. For a particular cybersecurity topic, AZSecure contains various data sets collected by researchers and practitioners with different backgrounds or interests, so it can support knowledge sharing and validation. As a result, users should perceive increased usefulness of AZSecure. Furthermore, instead of housing "only network traffic or malware related data," AZSecure accentuates its integration affordance by providing a rich array of cybersecurity-related data, "such as social media, that can generate deep and novel insights" (p. 2) [48]. Thus, we hypothesize:

H3: Integration affordance of AZSecure is positively related to its (a) ease of use and (b) usefulness, as perceived by users.

Perceived value, as a second-order formative construct, features four dimensions: financial, emotional, quality, and social value [52]. Both perceived ease of use and usefulness positively relate to perceived value that results from cognitive comparisons of gains versus losses associated with the use of a technology artifact or product [59]. Perceived ease of use influences individuals' cost evaluations, and costs (e.g., time, effort) determine their value assessments [29]. Because AZSecure provides easily accessible cybersecurity data, free of financial cost, it reduces users' efforts and psychological burdens (e.g., anxiety, frustration) [51]. As Kim et al. [29] explain, perceived usefulness constitutes a value determinant, reflecting users' benefit evaluation derived from a value assessment. For ISI, AZSecure, a well-designed OADR that contains detailed meta-data about each data set (such as structure and affiliated authors [48]), should increase individuals' assessments of its data content quality and value [19]. Therefore, we hypothesize:

H4: The (a) ease of use and (b) usefulness of AZSecure, as perceived by users, relate positively to their perception of its value.

The relationship of perceived value with intention to use might reflect two pathways. First, perceived value, similar to attitude toward adopting and using a technology artifact [24, 37], reflects the user's assessment of the artifact, positive or negative. The effort required to establish positive or negative evaluations may lay a foundation for cognitive comparisons that shape perceived value. In this vein, we expect a relationship between perceived value and user adoption. Second, the link between perceived value and user adoption appears in various technology contexts, including digital services [29, 52]. As an OADR, AZSecure offers data and related services to users, so we anticipate an effect of perceived value on their intentions to use.

Furthermore, the perceived value of AZSecure should affect users' intentions to collaborate in its use. To illustrate, the emotional dimension of perceived value reveals the enjoyment that a

user expects from using AZSecure, and enjoyment can influence collaboration (sharing) intentions and increase knowledge dissemination efforts [27]. When evaluating an OADR, people also might link the quality element of perceived value to trust and transparency [26], such that they could be more likely to trust the source when it provides better quality or more valid contents. In turn, perceived quality value should lay a foundation for collaboration. In addition, the social dimension of perceived value also implies the use of AZSecure meets social needs, such as social acceptance and reputation. Because AZSecure enforces guidelines for data set citations, users should perceive more social values from its data sets, credit data publishers, and collaborate with others (including publishers) in using these data. We therefore hypothesize:

H5: The value of AZSecure, as perceived by users, relates positively to their (a) intentions to use it and (b) intentions to collaborate with it.

5 STUDY DESIGN

To test the model and hypotheses, we performed a survey study that targets potential users of AZSecure (i.e., ISI researchers and practitioners), and recruited them from **Amazon Mechanical Turk (AMT).** We used three criteria to ensure responses from qualified participants, in line with previous research [35]. First, participants must reside in the United States and have an approval rate greater than 95%. Second, they must currently work in information technology areas. Third, we used a pre-survey screening to confirm their potential uses of AZSecure.[6]

The survey included two stages. First, participants were directed to AZSecure and asked to spend at least 30 minutes to learn and become familiar with this data repository, its design, features, structure, and contents. Second, they answered survey questions according to their evaluations and perceptions of AZSecure. The survey also had five attention and familiarity check questions (see Appendix A), and only those who answered at least three questions correctly were included in the subsequent analyses.

We measured the constructs with question items adapted from previously validated scales, with minor changes to fit the study context. Specifically, we operationalized usefulness and ease of use with items from Davis [13], intention to use from Venkatesh [54], and intention to collaborate from Turel et al. [53]. In line with Sheth et al. [49] and Ruiz et al. [45], we considered perceived value as a second-order formative construct and operationalized it with items adapted from Turel et al. [52]. For the accessibility, relevance, and integration affordances, we relied on items adapted from Nelson et al. [38]. All question items employed a 7-point Likert scale, with 1 indicating "strongly disagree" and 7 denoting "strongly agree." Three experienced ISI researchers reviewed the measurement items to ensure their face validity. We also collected each participant's demographic information as well as general computer and Internet skills, which were used as control variables in the analyses. Appendix B lists all the measurement items and their source(s).

6 ANALYSES AND RESULTS

As described, qualified participants examined AZSecure's design and contents, then provided their evaluative responses by answering questions regarding the respective constructs. A total of 240 ISI professionals took part in the study; among them, 224 passed the attention and familiarity check and completed the survey successfully. Table 3 provides descriptive statistics of the participants. Next, we examined the validity of the measurement model and then performed structural model analyses to test the hypotheses.

[6]The pre-survey screening has three criteria: exhibiting interest in ISI-related work or research, currently conducting ISI-related work or research, and having some experiences in ISI-related work or research. Participants must meet one of these criteria in order to participate in the survey study.

Table 3. Descriptive Statistics of Participants

Variable	Category	Percentage
Gender	Male	73.7%
	Female	26.3%
Age	18–24 years old	6.7%
	25–34 years old	40.2%
	35–44 years old	34.8%
	45–54 years old	14.3%
	55–64 years old	3.6%
	65–74 years old	0.4%
Work experience	<6 months	1.8%
	6–12 months	1.8%
	1–3 years	10.3%
	4–6 years	12.5%
	>7 years	73.7%
General computer skills	Novice (Very Poor – Somewhat Poor)	0.0%
	Intermediate (Fair)	1.8%
	Expert (Somewhat Good – Very Good)	98.3%
General Internet skills	Novice (Very Poor – Somewhat Poor)	0.4%
	Intermediate (Fair)	0.9%
	Expert (Somewhat good – Very good)	98.7%

We used SmartPLS 3 to test the measurement and structural models. We chose **partial least square structural equation modeling (PLS-SEM)** over other methods, such as **ordinary least squares (OLS)** and covariance-based SEM, because it is more appropriate for testing a model that contains both formative and reflective constructs [22]. Moreover, PLS-SEM is a nonparametric method that is robust to biases created by potential assumption violations (e.g., normality) that might arise due to the sample size.

6.1 Measurement Model Assessments

We assessed the measurement model with three efforts, in line with previous IS studies involving second-order formative constructs [52]. First, we examined all the reflective first-order constructs in terms of reliability and convergent and discriminant validity. After removing five question items with problematic item-level loadings and cross-loading [34], we assessed the (remaining) items' construct reliability, according to the Cronbach's alpha and composite reliability values, using a common threshold of 0.70 [22].[7] To establish convergent validity, the **average variance extracted (AVE)** for each construct should exceed 0.50 [22]. We used both Fornell-Larcker criteria and cross-loadings to examine discriminant validity [23]; the square root of the AVE for each latent variable should be greater than the pairwise correlations between any constructs. As we summarize in Table 4 and 5, all the criteria were satisfied in this initial analysis of the first-order measurement model (see Appendix C for the cross-loading details).

[7]Because we used previously validated measurement scales, item-level loadings should exceed 0.80 and exhibit at least a 0.20 difference in cross-loadings to ensure that items load substantially higher on their own construct than on other constructs [34].

Table 4. Construct Reliability and Convergent Validity

	Mean	Standard Deviation	Cronbach's Alpha	Composite Reliability	AVE
BI	4.89	1.44	0.97	0.98	0.94
CI	4.61	1.39	0.93	0.95	0.87
ACA	5.87	0.95	0.87	0.92	0.79
INA	5.85	0.89	0.80	0.91	0.84
REA	5.34	1.08	0.87	0.94	0.88
PEU	5.71	0.91	0.88	0.92	0.73
PEV	4.93	1.28	0.82	0.92	0.85
PFV	5.64	1.09	0.87	0.92	0.80
PQV	5.51	1.12	0.89	0.95	0.90
PSV	4.13	1.35	0.92	0.94	0.80
PU	5.12	1.25	0.95	0.96	0.84

Note. BI = intention to use; CI = intention to collaborate; ACA = accessibility affordance; INA = integration affordance; REA = relevance affordance; PEU = perceived ease of use; PU = perceived usefulness; PEV = perceived emotional value; PQV = perceived quality value; PFV = perceived financial value; PSV = perceived social value; AVE = Average Variance Extracted.

Table 5. Discriminant Validity Assessment

	BI	CI	ACA	INA	REA	PEU	PEV	PFV	PQV	PSV	PU
BI	**0.97**										
CI	0.56	**0.93**									
ACA	0.32	0.24	**0.89**								
INA	0.36	0.22	0.56	**0.87**							
REA	0.49	0.36	0.45	0.39	**0.94**						
PEU	0.33	0.28	0.60	0.46	0.44	**0.86**					
PEV	0.60	0.51	0.42	0.47	0.49	0.41	**0.92**				
PFV	0.14	0.10	0.34	0.31	0.21	0.37	0.30	**0.89**			
PQV	0.52	0.39	0.53	0.52	0.44	0.50	0.66	0.26	**0.93**		
PSV	0.42	0.47	0.26	0.19	0.40	0.25	0.57	0.23	0.48	**0.89**	
PU	0.58	0.45	0.33	0.43	0.48	0.33	0.49	0.07	0.58	0.41	**0.91**

Note. BI = intention to use; CI = intention to collaborate; ACA = accessibility affordance; INA = integration affordance; REA = relevance affordance; PEU = perceived ease of use; PU = perceived usefulness; PEV = perceived emotional value; PQV = perceived quality value; PFV = perceived financial value; PSV = perceived social value.

Second, we examined **common method bias (CMB).** According to Harman's single-factor test, a single-factor model only accounts for 36.51% of variance, suggesting that CMB is not a serious concern. As further support for this result, we adopted the smallest positive correlation of items [25] and again observed that CMB is not significant, because the confidence interval of the smallest positive correlation (between PFV2 and CI2) contains 0; i.e., 95% confidence interval = [−0.123, 0.141]. Next, we performed a full collinearity assessment [31], in which a **variance inflation factor (VIF)** greater than 3.3 would indicate problematic collinearity and signify that the model may be contaminated by CMB, whereas the model is free of CMB if all VIFs are below this level. We conducted 11 PLS factor analyses, in which one latent variable represented the dependent variable at a time. As we summarize in Table 6, all the collinearity statistics (factor-level VIFs) are below the suggested threshold (3.3), so CMB appears not a severe problem.

Table 6. Full Collinearity Statistics

VIF	BI	CI	ACA	INA	REA	PEU	PEV	PFV	PQV	PSV	PU
BI	-	1.96	2.13	2.13	2.07	2.12	2.01	2.11	2.12	2.13	1.98
CI	1.56	-	1.68	1.68	1.69	1.68	1.64	1.68	1.68	1.63	1.67
ACA	2.00	1.98	-	1.83	1.96	1.79	2.01	1.98	1.93	1.99	2.00
INA	1.88	1.84	1.69	-	1.87	1.82	1.81	1.78	1.82	1.88	1.78
REA	1.66	1.70	1.66	1.71	-	1.67	1.70	1.71	1.69	1.68	1.66
PEU	1.83	1.81	1.63	1.83	1.80	-	1.83	1.74	1.78	1.81	1.83
PEV	2.46	2.53	2.61	2.51	2.59	2.60	-	2.58	2.36	2.40	2.58
PFV	1.29	1.29	1.28	1.26	1.29	1.24	1.28	-	1.29	1.25	1.25
PQV	2.50	2.50	2.42	2.49	2.50	2.47	2.26	2.53	-	2.44	2.31
PSV	1.75	1.65	1.76	1.68	1.71	1.71	1.61	1.71	1.69	-	1.74
PU	1.91	2.02	2.04	1.95	1.99	2.05	2.03	2.02	1.88	2.02	-

Note. BI = intention to use; CI = intention to collaborate; ACA = accessibility affordance; INA = integration affordance; REA = relevance affordance; PEU = perceived ease of use; PU = perceived usefulness; PEV = perceived emotional value; PQV = perceived quality value; PFV = perceived financial value; PSV = perceived social value; VIF = Variance Inflation Factor.

Table 7. Formative Validity Assessment of Perceived Value

	PFV	PEV	PQV	PSV
Weight	0.18	0.27	0.40	0.43
t-value (2,000 resamples)	4.83	19.75	19.97	22.33
VIF	1.24	2.16	2.32	1.57

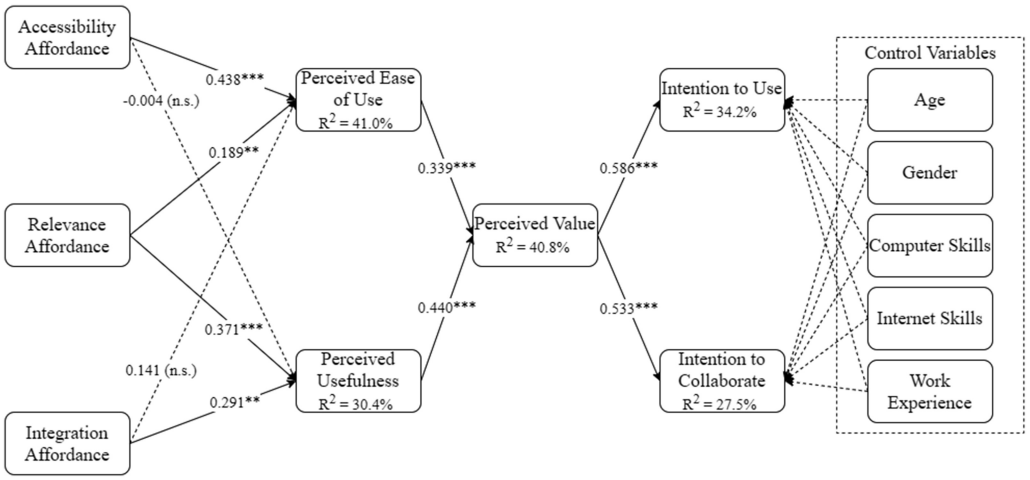
Note. VIF = variance inflation factor; PEV = perceived emotional value; PQV = perceived quality value; PFV = perceived financial value; PSV = perceived social value.

Third, we used the repeated indicator approach [34] to estimate perceived value, a second-order formative construct that contains all first-order constructs: perceived financial value, emotional value, quality value, and social value. We then assessed the validity of this second-order formative construct in two ways [34]. To qualify as a second-order formative construct, the weight of each lower-order construct that contributes to the higher-order construct should demonstrate a significant *t*-value. In addition, formative validity can be established by confirming the nonexistence of multicollinearity among first-order constructs, using the VIF with a common cutoff of 3.3. As Table 7 shows, perceived value met all these criteria, in further support of our conceptualization of a second-order formative construct.

6.2 Hypothesis Test Results

We used PLS-SEM to test the model and hypotheses, as it is appropriate for relatively small samples that may contest normality distributions [34]. We assessed the model's explanatory power by examining the R^2 value of the dependent variables. As shown in Figure 3, the results indicate that the model accounts for a significant amount of variance in each variable: perceived ease of use (41.0%), perceived usefulness (30.4%), perceived value (40.8%), intention to use (34.2%), and intention to collaborate (27.5%).

We employed bootstrapping with 1,000 resamples to estimate the significance of the path coefficients and found support for most of the hypotheses. Accessibility affordance relates to perceived ease of use significantly and positively (path coefficient = 0.438, $p < 0.001$), in support of H1a.



Note. ***p < .001; **p < .01; *p < .05; n.s. = not significant.

Fig. 3. Structural model test results.

However, its effect on perceived usefulness is not statistically significant (path coefficient = −0.004, $p > 0.05$), not confirming H1b. Relevance affordance has significant, positive effects on both perceived ease of use (path coefficient = 0.189, $p < 0.01$) and usefulness (path coefficient = 0.398, $p < 0.001$), in support of both H2a and H2b. Perceived usefulness relates significantly to integration affordance (path coefficient = 0.291, $p < 0.01$), and the relationship between perceived ease of use and integration affordance is insignificant (path coefficient = 0.141, $p > 0.05$). Thus, the data support H3b but not H3a. Perceived value relates significantly to both perceived ease of use (path coefficient = 0.339, $p < 0.001$) and perceived usefulness (path coefficient = 0.440, $p < 0.001$); that is, the results confirm H4a and H4b. Finally, perceived value has a significant, positive relationship with intention to use (path coefficient = 0.586, $p < 0.001$) and collaborate (path coefficient = 0.533, $p < 0.001$), in support of H5a and H5b. The control variables have no significant effects on the two dependent variables.

Our results affirm the importance of context-specific factors and reveal indirect paths through which the essential affordances of an OADR influence individuals' intentions to use and collaborate. Relevance affordance has significant, indirect effects on both usage and collaboration intentions, through perceived ease of use and perceived usefulness (Table 8). The relationships of accessibility affordance with both usage and collaboration intentions seem to funnel solely through perceived ease of use. Integration affordance instead relates to these intentions significantly and indirectly through perceived usefulness. Jointly, these results reveal the important mediating roles of perceived usefulness and ease of use in the relationships of different affordances with usage and collaboration intentions.

To establish the significance of these indirect effects, we also conducted an *ex post* assessment of an OLS model that has only direct relationships of the predictors with individual intentions to use and collaborate. As shown in Table 9, the results confirm the significance of perceived value for predicting both usage and collaboration intentions, but perceived ease of use is insignificant. None of the affordances is significantly related to individual intentions to use or collaborate except for relevance affordance. The comparative results affirm the value of including indirect effects to explain user intentions more fully.

Finally, we conducted a comparative analysis and observed substantial differences between adopters and non-adopters, as well as between collaborators and non-collaborators. First, we split

Table 8. Indirect Path Analysis Results

Indirect Path	Effect	Lower 2.5%	Upper 97.5%	Significance?
ACA → PEU → PV → CI	0.079	0.036	0.127	Yes
ACA → PEU → PV → BI	0.087	0.042	0.133	Yes
ACA → PU → PV → CI	−0.001	−0.039	0.034	No
ACA → PU → PV → BI	−0.001	−0.041	0.036	No
INA → PEU → PV → CI	0.025	−0.004	0.067	No
INA → PEU → PV → BI	0.028	−0.004	0.072	No
INA → PU → PV → CI	0.068	0.020	0.121	Yes
INA → PU → PV → BI	0.075	0.021	0.133	Yes
REA → PEU → PV → CI	0.034	0.006	0.066	Yes
REA → PEU → PV → BI	0.037	0.006	0.070	Yes
REA → PU → PV → CI	0.087	0.041	0.152	Yes
REA → PU → PV → BI	0.096	0.042	0.168	Yes

Note. BI = intention to use; CI = intention to collaborate; ACA = accessibility affordance; INA = integration affordance; REA = relevance affordance; PEU = perceived ease of use; PU = perceived usefulness; PV = perceived value.

Table 9. Results of OLS Regression Model with Direct Effects Only

Predictor (Beta)	DV1: Intention to Use	DV2: Intention to Collaborate
Affordances of OADR in ISI:		
ACA	−0.029	−0.046
INA	0.021	−0.105
REA	0.185**	0.099
User Perceptions:		
PU	0.327***	0.224**
PEU	0.022	0.051
PV	0.305***	0.406***
Control Variables:		
Computer Skills	−0.014	−0.134
Internet Skills	−0.094	0.069
Gender	−0.045	−0.005
Age	−0.005	0.005
Work Experience	0.038	0.038
Model Summary:		
R^2	46.6%	32.5%

Note. ACA = accessibility affordance; INA = integration affordance; REA = relevance affordance; PEU = perceived ease of use; PU = perceived usefulness; PEV = perceived emotional value; PV = perceived value. ***p < .001; **p < .01; *p < .05.

the participants into two subgroups, according to their indicated intentions to use or to collaborate (a dependent variable).[8] Among the participants, 45 are non-adopters (20.1%) and 55 are non-collaborators (24.6%). For each dependent variable, we performed ANOVA tests to compare

[8]Participants with a latent variable score less than 4 for the "intention to use" construct were considered as non-adopters and those with a score greater than 4 were considered as adopters. Similarly, we used participants' latent variable scores for the "intention to collaborate" construct to separate collaborators and non-collaborators; i.e., less versus greater than 4 in the score.

Table 10. Comparative Analysis of Adopters/Collaborators vs. Non-adopters/Non-collaborators

Construct	ADTs	Non-ADTs	ANOVA F: ADTs vs. Non-ADTs	COTs	Non-COTs	ANOVA F: COTs vs. Non-COTs
PSV	4.37	3.19	30.74***	4.41	3.28	32.58***
PEV	5.2	3.87	46.54***	5.21	4.09	37.03***
PU	5.42	3.95	63.6***	5.35	4.4	27.10***
REA	5.53	4.57	32.9***	5.49	4.86	14.85***
PQV	5.57	4.7	33.81***	5.68	4.97	17.93***
PEU	5.79	5.43	5.65*	5.79	5.47	5.21*
INA	5.93	5.52	7.79**	5.87	5.78	0.42
ACA	5.95	5.53	7.5**	5.93	5.67	3.12
PFV	5.66	5.57	0.2	5.63	5.66	0.03

Note. ADTs = Adopters; Non-ADTs = Non-adopters; COTs = Collaborators; Non-COTs = Non-collaborators; ACA = accessibility affordance; INA = integration affordance; REA = relevance affordance; PEU = perceived ease of use; PU = perceived usefulness; PEV = perceived emotional value; PQV = perceived quality value; PFV = perceived financial value; PSV = perceived social value. ***$p < .001$; **$p < .01$; *$p < .05$.

the two subgroups, adopters versus non-adopters or collaborators versus non-collaborators, by examining the latent variable score of each construct. As we show in Table 10, adopters and non-adopters of AZSecure substantially differ in their responses for each construct, with the exception of PFV. Moreover, the analysis shows that overall evaluations of AZSecure by adopters versus non-adopters are significantly influenced by three constructs: PSV (1.18 in difference), PEV (1.33 in difference) and PU (1.47 in difference). Similarly, participants' responses regarding these three constructs (i.e., PSV, PEV, PU) also separate the evaluations of AZSecure by collaborators versus non-collaborators.

7 DISCUSSION

This study demonstrates the value and feasibility of combining essential affordances of OADRs and user perceptions to explain ISI professionals' intentions to use and collaborate. The affordance constructs represent less subjective and more utilitarian variables for assessing the value of an OADR. They also enable users to evaluate an OADR in terms of its practical value and the decision to adopt and use the provided data sets. This study serves as a point of departure for examining uses of OADRs and sheds light on the importance of affordance and user perceptions by combining user acceptance and value assessment perspectives, rather than relying on a dominant reliance on user perceptions, as in many previous studies.

This study also suggests a promising approach to analyze user adoption in unique, professional contexts. Prevalent models consider many general benefits [4, 26, 55]; our approach emphasizes a utilitarian orientation and context specificity, highlighting the need to consider what a technology artifact can afford people to do. The results show that relevance affordance of OADRs is a crucial determinant of user adoption, through increased usefulness, ease of use, and value perceived by users. Not all affordances of an OADR are equally important though. Accessibility affordance, supported by metadata and catalogs, does not appear to increase perceived value but can heighten perceived ease of use, and thus contributes to the perceived value associated with adoption. This is probably because, when ISI professionals assess whether to adopt AZSecure, they consider not only its design, accessibility, and structure for organizing and delivering contents, but also the content richness in breadth, depth, and recency. That is, the affordance of easy access cannot always guarantee the contents are appropriate and useful for individuals' needs, so its effects on perceived usefulness may decrease due to ISI researchers and practitioners need to perform

various tasks and activities. In a related sense, integrating data from different sources encourages user adoption through increased usefulness perceptions, but it might not affect perceived ease of use. This perhaps is because integrating various, vast amounts of data may lead individuals to perceive information overload and increased complexity, which diminishes the significance of integration affordance's positive effect on perceived ease of use. These findings help augment user adoption and behavior research in professional contexts (e.g., ISI, healthcare); they may benefit future research by implying the differential roles of affordances in user adoption.

Unlike existing literature that focuses on perceived value exclusively [6, 29, 52], this study considers its interplay with important user acceptance antecedents. Both perceived ease of use and usefulness influence users' perceptions of an OADR's value for their analyses and tasks, which may benefit user adoption research by demonstrating the importance of user value assessments in public domains in which technology artifacts are free of cost. In addition to the usability of a technology artifact, individuals' adoptions of open resources and tools seem affected by their value assessments, such as data quality and social values. As shown in Table 10, the importance of value assessments is evident in the comparative analysis between adopters and non-adopters, as well as between collaborators and non-collaborators. Individual perceptions of emotional and social value appear to be important reasons why ISI professionals choose not to adopt and collaborate using AZSecure. In turn, these findings signify the significance of emotional and social support by an OADR to favorably influence targeted users' adoption decisions, which represents a promising future research direction.

Furthermore, this study has implications for ISI practices. For example, the significance of particular affordances can provide design guidelines for OADRs in ISI. As we demonstrate, the design of an OADR should emphasize accessibility affordance to encourage its adoption and use by ISI professionals, such as providing metadata, intuitive navigation tools, and search capabilities. To increase usefulness, an OADR should offer integration (e.g., tools for dealing with multilingual data sets) and relevance (e.g., ReadMe files, recommended analyses) affordances. Also, people's value assessments inform their usage and collaboration intentions; social value might be especially important to novice users. In this vein, OADRs should highlight their data and promote the image and status of individual professionals within the ISI community. Moreover, the evidence we obtain about collaboration intentions suggests that the use of OADRs can foster collaborations among ISI professionals for effective knowledge reproducibility and discoverability, in addition to their individual tasks and activities. AZSecure encourages user collaboration by enacting restrictions on how to cite data sets provided by others. Virtual venues for communications and exchanges could support insightful discussions and timely knowledge dissemination too, as a promising extension of existing OADRs. To illustrate, AZSecure can host discussion forums that enable ISI professionals to interact and get help from others, so they would develop a greater emotional attachment. In addition, the use of gamification design elements (e.g., competition, badge) may facilitate users' internalization of social value, which help them form a strong bond with AZSecure. Finally, cybersecurity organizations and governmental funding agencies should strive to evaluate the impacts of their investments and resource-intensive efforts to build OADRs. An affordance perspective may help these organizations make more informed investment decisions. For example, conducting a low-cost affordance survey of ISI professionals could be beneficial in establishing prioritization for alternative OADR projects.

8 CONCLUSION

This study identifies important factors that influence adoptions of OADRs by ISI researchers and practitioners. The results indicate that accessibility, relevance, and integration, as three unique affordances, can promote ISI professionals' usage and collaboration intentions, through perceived

ease of use, usefulness, and value. This study makes several contributions to ISI research and practice. First, we identify three affordances unique to OADRs for the ISI community, in light of essential data requirements. For affordance literature [36, 42], we reveal specific affordances. Second, using the lens of affordance, we theorize relationships across user acceptance antecedents and value assessments, and specify how their interplay can explain users' intentions to use an OADR and collaborate with it. The findings help clarify the underlying mechanisms by which affordances influence individual usage and collaboration intentions, so they can move beyond research that concentrates on either user acceptance or value assessment perspectives to explain user adoption of a technology artifact. Third, this study contributes to the ISI community by shedding light on effective OADR designs and highlighting collaborations as a crucial objective for developing them.

This study also has several limitations that deserve further research attention. First, this study examines the perceptions of ISI researchers and practitioners recruited from Amazon Mechanical Turk, and produces results suggesting several key factors that jointly determine their intentions to use and collaborate with AZSecure. This study represents a precursory assessment of potential users' adoptions, thus enabling future research to further analyze ISI professionals' adoptions and continuous uses of AZSecure more fully. While this study targets potential users of AZSecure, we acknowledge that users often differ in their focus and objective, so other professionals may have different value perceptions of an OADR. Future investigations of different user groups could unfold interesting distinctions and means for improved designs and usages. Second, our study focuses on theorization and empirical test; hence, future research can use qualitative methods (e.g., interview, case study) to identify important reasons why ISI researchers and practitioners choose not to adopt AZSecure and thus shed new insights on how to grow the user base by profiling adopters versus non-adopters according to individual characteristics, past experiences, areas of interest, frequently accessed contents, focus, and objectives. In addition, while we use perceived value to explain collaboration intention, future research should consider additional factors, such as social influences, trust, and risk. Although we gather survey data to assess ISI professionals' intentions to use and collaborate, behavioral data can offer an alternative and supplementary view of affordance theory in the ISI context. Finally, this study analyzes user assessments and perceptions, not their interactions, which represents another direction to further examine user adoption of OADRs.

APPENDICES

A ATTENTION AND FAMILIARITY CHECK QUESTIONS

1: Which of the following types of data sets is NOT included in AZSecure?
   a. Web forums
   b. Internet phishing websites
   c. Internet relay chat
   d. DARPA Intrusion Detection

2: Which of the following forum data sets is NOT available in AZSecure's "Other Forums" category?
   a. CrackingArena Forum
   b. Zhihu Forum
   c. Baidu Forum
   d. Douban Group

3: Which of the following the organization types is NOT included in AZSecure's "Internet Phishing Websites" category?
   a. Financial
   b. Pharmacy

c. Public School
d. Targeted Brands
4: Which of the following languages is NOT included in AZSecure's "Dark Web Forums" category?
a. English
b. Arabic
c. Russian
d. Spanish
5: Which of following countries is NOT included in AZSecure's "GeoWeb Forums" category?
a. AFGHANISTAN
b. PAKISTAN
c. CHINA
d. IRAQ

B SUMMARY OF MEASUREMENT ITEMS USED IN THIS STUDY

Demographic Variables:
Age: 18–24, 25–34, 35–44, 45–54, 55–64, 65–74, >75 years older
Gender: Male or Female
Work experience: <6 months, 6–12 months, 1–3 years, 4–6 years, >7 years
General computer skills: How would you evaluate your computer skills in general? (1 = Very Poor, 7 = Very Good)
General Internet skills: How would you evaluate your Internet (Web) skills in general? (1 = Very Poor, 7 = Very Good)

Perceived Usefulness (PU), [13]
PU1: Using AZSecure would enable me to do my job more quickly.
PU2: Using AZSecure would improve my performance for doing my job.
PU3: Using AZSecure would increase my productivity for doing my job.
PU4: Using AZSecure would enhance my effectiveness for doing my job.
PU5: I would find AZSecure useful for my job.

Perceived Ease of Use (PEU), [13]
PEU1: Learning to use AZSecure would be easy for me.
PEU2: I would find it easy to get data from AZSecure to do what I want it to do.
PEU3: My interaction with AZSecure would be clear and understandable.
PEU4: I would find AZSecure easy to use.
PEU5: I would find AZSecure to be flexible to interact with. (Dropped)
Intention to Use (BI), [54]
BI1: I intend to use AZSecure in near future.
BI2: I predict that I would use AZSecure in near future.
BI3: I plan to use AZSecure in near future.

Intention to Collaborate (CI), [53]
CI1: Assuming I can connect with others who use AZSecure, I intend to use it for group research projects.
CI2: Given that I can connect with others who use AZSecure, I predict that I would use it to collaborate with others.
CI3: If I can connect to others who use AZSecure, I plan to use it for future collaboration.

Integration Affordance (INA), [38]
IG1: AZSecure effectively combines data from different areas.

IG2: AZSecure pulls together information that comes from different places.
IG3: AZSecure effectively integrates data from different areas.

Relevance Affordance (REA), [38]
IR1: AZSecure provides information that is relevant to my needs.
IR2: AZSecure provides information that is consistent with my purposes.
IR3: AZSecure is missing critical information that would be very useful to me. (Dropped)

Accessibility Affordance (ACA), [38]
IA1: AZSecure allows information to be readily accessible to me.
IA2: AZSecure makes information very accessible.
IA3: AZSecure makes information easy to access.

Perceived Quality Value (PQV), [52]
PQV1: Overall, I would give AZSecure high marks.
PQV2: Overall, I would give AZSecure a high rating in terms of quality.
PQV3: Overall, AZSecure is of high quality.

Perceived Emotional Value (PEV), [52]
PEV1: AZSecure is the one that I feel relaxed about using.
PEV2: The use of AZSecure makes me feel good.
PEV3: AZSecure is the one that I enjoy. (Dropped)
PEV4: AZSecure makes me want to use them. (Dropped)

Perceived Financial Value (PFV), [52]
PFV1: AZSecure is economical.
PFV2: AZSecure offers value for money.
PFV3: AZSecure is good relative to the cost of use.
PFV4: The cost of using AZSecure is low. (Dropped)

Perceived Social Value (PSV), [52]
PSV1: The use of AZSecure helps me feel acceptable.
PSV2: The use of AZSecure improves the way I am perceived.
PSV3: The fact that I use AZSecure makes a good impression on other people.
PSV4: The use of AZSecure gives me social approval.

C CROSS-LOADINGS OF FIRST-ORDER CONSTRUCTS

	BI	CI	ACA	INA	REA	PEU	PEV	PFV	PQV	PSV	PU
BI1	**0.97**	0.55	0.32	0.33	0.47	0.29	0.58	0.12	0.50	0.42	0.56
BI2	**0.96**	0.52	0.32	0.38	0.47	0.35	0.59	0.15	0.53	0.38	0.57
BI3	**0.97**	0.55	0.30	0.33	0.49	0.31	0.56	0.14	0.48	0.42	0.57
CI1	0.49	**0.91**	0.17	0.14	0.31	0.18	0.46	0.08	0.32	0.47	0.40
CI2	0.53	**0.95**	0.23	0.21	0.34	0.28	0.47	0.10	0.37	0.40	0.41
CI3	0.54	**0.94**	0.27	0.25	0.36	0.30	0.50	0.11	0.41	0.44	0.44
IA1	0.31	0.19	**0.90**	0.49	0.45	0.60	0.41	0.31	0.47	0.20	0.33
IA2	0.28	0.21	**0.89**	0.49	0.40	0.46	0.38	0.32	0.45	0.22	0.26
IA3	0.27	0.23	**0.88**	0.50	0.35	0.52	0.34	0.27	0.48	0.27	0.27
IG1	0.27	0.17	0.39	**0.86**	0.27	0.36	0.32	0.26	0.41	0.10	0.34
IG2	0.23	0.14	0.51	**0.88**	0.29	0.41	0.36	0.28	0.37	0.10	0.33
IG3	0.41	0.25	0.54	**0.88**	0.44	0.43	0.53	0.27	0.55	0.27	0.45
IR1	0.49	0.33	0.41	0.35	**0.94**	0.39	0.47	0.16	0.38	0.39	0.44
IR2	0.44	0.35	0.44	0.38	**0.95**	0.43	0.46	0.24	0.45	0.36	0.47
PEU1	0.30	0.22	0.47	0.30	0.33	**0.85**	0.31	0.32	0.38	0.19	0.30
PEU2	0.32	0.29	0.54	0.45	0.43	**0.86**	0.39	0.32	0.47	0.23	0.33
PEU3	0.22	0.18	0.49	0.40	0.34	**0.85**	0.29	0.31	0.40	0.17	0.20
PEU4	0.28	0.24	0.55	0.40	0.39	**0.87**	0.41	0.33	0.46	0.25	0.30
PEV1	0.55	0.48	0.41	0.45	0.45	0.44	**0.93**	0.30	0.65	0.48	0.46
PEV2	0.55	0.47	0.37	0.42	0.45	0.31	**0.92**	0.25	0.56	0.57	0.43
PFV1	0.12	0.12	0.33	0.28	0.20	0.32	0.30	**0.92**	0.28	0.23	0.08
PFV2	0.12	0.04	0.23	0.29	0.11	0.27	0.21	**0.82**	0.15	0.21	0.06
PFV3	0.14	0.10	0.33	0.27	0.24	0.39	0.29	**0.93**	0.26	0.19	0.05
PQV1	0.52	0.35	0.50	0.52	0.47	0.47	0.59	0.26	**0.91**	0.42	0.58
PQV2	0.47	0.39	0.50	0.48	0.39	0.49	0.62	0.24	**0.96**	0.46	0.55
PQV3	0.47	0.36	0.46	0.45	0.38	0.45	0.64	0.23	**0.93**	0.47	0.50
PSV1	0.39	0.37	0.27	0.17	0.39	0.23	0.54	0.25	0.43	**0.83**	0.39
PSV2	0.40	0.45	0.18	0.14	0.36	0.17	0.51	0.19	0.38	**0.92**	0.37
PSV3	0.39	0.42	0.27	0.22	0.33	0.25	0.51	0.18	0.51	**0.91**	0.39
PSV4	0.34	0.44	0.19	0.15	0.34	0.23	0.47	0.20	0.38	**0.91**	0.32
PU1	0.56	0.43	0.31	0.39	0.40	0.30	0.44	-0.01	0.50	0.39	**0.92**
PU2	0.57	0.44	0.30	0.38	0.43	0.31	0.47	0.08	0.57	0.40	**0.92**
PU3	0.55	0.44	0.29	0.39	0.44	0.32	0.46	0.10	0.55	0.41	**0.93**
PU4	0.49	0.39	0.29	0.38	0.47	0.31	0.46	0.06	0.56	0.34	**0.92**
PU5	0.51	0.34	0.30	0.45	0.45	0.28	0.39	0.07	0.48	0.34	**0.89**

Note. BI = intention to use; CI = intention to collaborate; ACA = accessibility affordance; INA = integration affordance; REA = relevance affordance; PEU = perceived ease of use; PU = perceived usefulness; PEV = perceived emotional value; PQV = perceived quality value; PFV = perceived financial value; PSV = perceived social value.

REFERENCES

[1] Ahmed Abbasi, Fatemeh Mariam Zahedi, and Siddharth Kaza. 2012. Detecting fake medical web sites using recursive trust labeling. *ACM Trans. Inf. Syst.* 30, 4 (November 2012), 1–36. DOI: https://doi.org/10.1145/2382438.2382441

[2] Ahmed Abbasi, Fatemeh Mariam Zahedi, Daniel Zeng, Yan Chen, Hsinchun Chen, and Jay F. Nunamaker. 2015. Enhancing predictive analytics for anti-phishing by exploiting website genre information. *J. Manag. Inf. Syst.* 31, 4 (January 2015), 109–157. DOI: https://doi.org/10.1080/07421222.2014.1001260

[3] Abbasi, Zhang, Zimbra, Chen, and Nunamaker. 2010. Detecting fake websites: The contribution of statistical learning theory. *MIS Q.* 34, 3 (February 2010), 435. DOI: https://doi.org/10.2307/25750686

[4] Mohammed Saleh Altayar. 2018. Motivations for open data adoption: An institutional theory perspective. *Gov. Inf. Q.* 35, 4 (October 2018), 633–643. DOI: https://doi.org/10.1016/j.giq.2018.09.006

[5] Mary Anne Kennan. 2011. Learning to share: Mandates and open access. *Libr. Manag.* 32, 4/5 (May 2011), 302–318. DOI: https://doi.org/10.1108/01435121111132301

[6] Aaron Baird and T. S. Raghu. 2015. Associating consumer perceived value with business models for digital services. *Eur. J. Inf. Syst.* 24, 1 (January 2015), 4–22. DOI: https://doi.org/10.1057/ejis.2013.12

[7] Victor Benjamin, Joseph S. Valacich, and Hsinchun Chen. 2019. DICE-E: A framework for conducting darknet identification, collection, evaluation with ethics. *MIS Q.* 43, 1 (January 2019), 1–22. DOI: https://doi.org/10.25300/MISQ/2019/13808

[8] Victor Benjamin, Bin Zhang, Jay F. Nunamaker, and Hsinchun Chen. 2016. Examining hacker participation length in cybercriminal internet-relay-chat communities. *J. Manag. Inf. Syst.* 33, 2 (April 2016), 482–510. DOI: https://doi.org/10.1080/07421222.2016.1205918

[9] Kelly Bissell, Ryan Lasalle, and Paolo Dal Cin. 2019. 2019 Cost of cybercrime study | 9th Annual | Accenture. Retrieved November 8, 2020 from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50.

[10] A. J. Burns, Tom L. Roberts, Clay Posey, and Paul Benjamin Lowry. 2019. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Inf. Syst. Res.* 30, 4 (December 2019), 1228–1247. DOI: https://doi.org/10.1287/isre.2019.0860

[11] Chen, Chiang, and Storey. 2012. Business intelligence and analytics: From big data to big impact. *MIS Q.* 36, 4 (2012), 1165. DOI: https://doi.org/10.2307/41703503

[12] Judy Chuan-Chuan Lin and Hsipeng Lu. 2000. Towards an understanding of the behavioural intention to use a web site. *Int. J. Inf. Manage* 20, 3 (June 2000), 197–208. DOI: https://doi.org/10.1016/S0268-4012(00)00005-0

[13] Fred D. Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* 13, 3 (September 1989), 319. DOI: https://doi.org/10.2307/249008

[14] Po-Yi Du, Ning Zhang, Mohammedreza Ebrahimi, Sagar Samtani, Ben Lazarine, Nolan Arnold, Rachael Dunn, Sandeep Suntwal, Guadalupe Angeles, Robert Schweitzer, and Hsinchun Chen. 2018. Identifying, collecting, and presenting hacker community data: Forums, IRC, Carding Shops, and DNMs. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE 70–75. DOI: https://doi.org/10.1109/ISI.2018.8587327

[15] Frankwell W. Dulle and M. K. Minishi-Majanja. 2011. The suitability of the Unified Theory of Acceptance and Use of Technology (UTAUT) model in open access adoption studies. *Inf. Dev.* 27, 1 (February 2011), 32–45. DOI: https://doi.org/10.1177/0266666910385375

[16] Mohammadreza Ebrahimi, Jay F. Nunamaker, and Hsinchun Chen. 2020. Semi-supervised cyber threat identification in dark net markets: A transductive and deep learning approach. *J. Manag. Inf. Syst.* 37, 3 (July 2020), 694–722. DOI: https://doi.org/10.1080/07421222.2020.1790186

[17] Mohammadreza Ebrahimi, Mihai Surdeanu, Sagar Samtani, and Hsinchun Chen. 2018. Detecting cyber threats in non-English dark net markets: A cross-lingual transfer learning approach. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE 85–90. DOI: https://doi.org/10.1109/ISI.2018.8587404

[18] Jenny Fry, Valérie Spezi, Stephen Probets, and Claire Creaser. 2016. Towards an understanding of the relationship between disciplinary research cultures and open access repository behaviors. *J. Assoc. Inf. Sci. Technol.* 67, 11 (November 2016), 2710–2724. DOI: https://doi.org/10.1002/asi.23621

[19] David Gefen. 2004. What makes an ERP implementation relationship worthwhile: Linking trust mechanisms and ERP usefulness. *J. Manag. Inf. Syst.* 21, 1 (January 2004), 263–288. DOI: https://doi.org/10.1080/07421222.2004.11045792

[20] James J. Gibson. 1977. *The Theory of Affordances.* Hilldale, USA.

[21] James J. Gibson. 1979. *The Ecological Approach to Visual Perception. Houghton, Mifflin and Company*, Boston, MA, US.

[22] Oliver Götz, Kerstin Liehr-Gobbers, and Manfred Krafft. 2010. Evaluation of structural equation models using the partial least squares (PLS) approach. In *Handbook of Partial Least Squares.* Springer Berlin, Berlin, Heidelberg, 691–711. DOI: https://doi.org/10.1007/978-3-540-32827-8_30

[23] Joe F. Hair, Marko Sarstedt, Christian M. Ringle, and Jeannette A. Mena. 2012. An assessment of the use of partial least squares structural equation modeling in marketing research. *J. Acad. Mark. Sci.* (2012). DOI: https://doi.org/10.1007/s11747-011-0261-6

[24] Paul J. Hu, Patrick Y. K. Chau, Olivia R. Liu Sheng, and Kar Yan Tam. 1999. Examining the technology acceptance model using physician acceptance of telemedicine technology. *J. Manag. Inf. Syst.* 16, 2 (September 1999), 91–112. DOI: https://doi.org/10.1080/07421222.1999.11518247

[25] Paul Jen-Hwa Hu, Han-fen Hu, Chih-Ping Wei, and Pei-Fang Hsu. 2016. Examining firms' green information technology practices: A hierarchical view of key drivers and their effects. *J. Manag. Inf. Syst.* 33, 4 (October 2016), 1149–1179. DOI: https://doi.org/10.1080/07421222.2016.1267532

[26] Marijn Janssen, Yannis Charalabidis, and Anneke Zuiderwijk. 2012. Benefits, adoption barriers and myths of open data and open government. *Inf. Syst. Manag.* 29, 4 (September 2012), 258–268. DOI: https://doi.org/10.1080/10580530.2012.716740

[27] Kankanhalli, Tan, and Wei. 2005. Contributing knowledge to electronic knowledge repositories: An empirical investigation. *MIS Q.* 29, 1 (2005), 113. DOI: https://doi.org/10.2307/25148670

[28] Maxat Kassen. 2013. A promising phenomenon of open data: A case study of the Chicago open data project. *Gov. Inf. Q.* 30, 4 (October 2013), 508–513. DOI: https://doi.org/10.1016/j.giq.2013.05.012

[29] Hee-Woong Kim, Hock Chuan Chan, and Sumeet Gupta. 2007. Value-based adoption of mobile internet: An empirical investigation. *Decis. Support Syst.* 43, 1 (February 2007), 11–126. DOI: https://doi.org/10.1016/j.dss.2005.05.009

[30] Michael Kistler, Serena Bonaretti, Marcel Pfahrer, Roman Niklaus, and Philippe Büchler. 2013. The virtual skeleton database: An open access repository for biomedical research and collaboration. *J. Med. Internet Res.* 15, 11 (November 2013), e245. DOI: https://doi.org/10.2196/jmir.2930

[31] Ned Kock. 2015. Common method bias in PLS-SEM. *Int. J. e-Collaboration* 11, 4 (October 2015), 1–10. DOI: https://doi.org/10.4018/ijec.2015100101

[32] Carrie K. W. Li, Thomas J. Holt, Adam M. Bossler, and David C. May. 2016. Examining the mediating effects of social learning on the low self-control—cyberbullying relationship in a youth sample. *Deviant Behav.* 37, 2 (February 2016), 126–138. DOI: https://doi.org/10.1080/01639625.2014.1004023

[33] Weifeng Li, Hsinchun Chen, and Jay F. Nunamaker. 2016. Identifying and profiling key sellers in cyber carding community: AZSecure text mining system. *J. Manag. Inf. Syst.* 33, 4 (October 2016), 1059–1086. DOI: https://doi.org/10.1080/07421222.2016.1267528

[34] Paul Benjamin Lowry and James Gaskin. 2014. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Trans. Prof. Commun.* 57, 2 (June 2014), 123–146. DOI: https://doi.org/10.1109/TPC.2014.2312452

[35] Paul Benjamin Lowry, Gregory D. Moody, and Sutirtha Chatterjee. 2017. Using IT design to prevent cyberbullying. *J. Manag. Inf. Syst.* 34, 3 (July 2017), 863–901. DOI: https://doi.org/10.1080/07421222.2017.1373012

[36] M. Lynne Markus and Mark Silver. 2008. A foundation for the study of IT effects: A new look at Desanctis and Poole's concepts of structural features and spirit. *J. Assoc. Inf. Syst.* 9, 10 (October 2008), 609–632. DOI: https://doi.org/10.17705/1jais.00176

[37] Kieran Mathieson. 1991. Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Inf. Syst. Res.* 2, 3 (September 1991), 173–191. DOI: https://doi.org/10.1287/isre.2.3.173

[38] R. Ryan Nelson, Peter A. Todd, and Barbara H. Wixom. 2005. Antecedents of information and system quality: An empirical examination within the context of data warehousing. *J. Manag. Inf. Syst.* 21, 4 (2005), 199–235. DOI: https://doi.org/10.1080/07421222.2005.11045823

[39] Irene V. Pasquetto, Bernadette M. Randles, and Christine L. Borgman. 2017. On the reuse of scientific data. *Data Sci. J.* 16, (March 2017). DOI: https://doi.org/10.5334/dsj-2017-008

[40] Fabio Pierazzi, Ghita Mezzour, Qian Han, Michele Colajanni, and V. S. Subrahmanian. 2020. A data-driven characterization of modern android spyware. *ACM Trans. Manag. Inf. Syst.* 11, 1 (April 2020), 1–38. DOI: https://doi.org/10.1145/3382158

[41] Stephen Pinfield, Jennifer Salter, Peter A. Bath, Bill Hubbard, Peter Millington, Jane H. S. Anders, and Azhar Hussain. 2014. Open-access repositories worldwide, 2005–2012: Past growth, current characteristics, and future possibilities. *J. Assoc. Inf. Sci. Technol.* 65, 12 (December 2014), 2404–2421. DOI: https://doi.org/10.1002/asi.23131

[42] Giulia Pozzi, Federico Pigni, and Claudio Vitari. 2014. Affordance theory in the IS discipline: A review and synthesis of the literature. In *20th Americas Conference on Information Systems*, AMCIS 2014. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01923663/document.

[43] Jialun Qin, Yilu Zhou, Edna Reid, Guanpi Lai, and Hsinchun Chen. 2007. Analyzing terror campaigns on the internet: Technical sophistication, content richness, and Web interactivity. *Int. J. Hum. Comput. Stud.* 65, 1 (January 2007), 71–84. DOI: https://doi.org/10.1016/j.ijhcs.2006.08.012

[44] Widia Resti Fitriani, Achmad Nizar Hidayanto, Puspa I. Sandhyaduhita, Betty Purwandari, and Meidi Kosandi. 2019. Determinants of continuance intention to use open data website: An insight from Indonesia. *Pacific Asia J. Assoc. Inf. Syst.* (2019), 96–120. DOI: https://doi.org/10.17705/1pais.11205

[45] David Martín Ruiz, Dwayne D. Gremler, Judith H. Washburn, and Gabriel Cepeda Carrión. 2008. Service value revisited: Specifying a higher-order, formative measure. *J. Bus. Res.* 61, 12 (December 2008), 1278–1291. DOI: https://doi.org/10.1016/j.jbusres.2008.01.015

[46] Sagar Samtani, Ryan Chinn, Hsinchun Chen, and Jay F. Nunamaker. 2017. Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *J. Manag. Inf. Syst.* 34, 4 (October 2017), 1023–1053. DOI: https://doi.org/10.1080/07421222.2017.1394049

[47] Iqbal H. Sarker, A. S. M. Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters, and Alex Ng. 2020. Cybersecurity data science: An overview from machine learning perspective. *J. Big Data* 7, 1 (December 2020), 41. DOI: https://doi.org/10.1186/s40537-020-00318-5

[48] Resha Shenandoah, Sagar Samtani, Mark Patton, and Hsinchun Chen. 2017. Fostering cybersecurity big data research: A case study of the AZSecure data system. Retrieved from http://sagarsamtani.com/wp-content/uploads/2018/07/Shenandoah-et-al-2017-Fostering-Big-Data-Cybersecurity-Research-2.pdf.

[49] Jagdish N. Sheth, Bruce I. Newman, and Barbara L. Gross. 1991. Why we buy what we buy: A theory of consumption values. *J. Bus. Res.* 22, 2 (March 1991), 159–170. DOI: https://doi.org/10.1016/0148-2963(91)90050-8.

[50] Diane Strong, Olga Volkoff, Sharon Johnson, Lori Pelletier, Bengisu Tulu, Isa Bar-On, John Trudel, and Lawrence Garber. 2014. A theory of organization-EHR affordance actualization. *J. Assoc. Inf. Syst.* 15, 2 (February 2014), 53–85. DOI: https://doi.org/10.17705/1jais.00353

[51] Heshan Sun and Ping Zhang. 2006. Causal relationships between perceived enjoyment and perceived ease of use: An alternative approach. *J. Assoc. Inf. Syst.* 7, 9 (September 2006), 618–645. DOI: https://doi.org/10.17705/1jais.00100

[52] Ofir Turel, Alexander Serenko, and Nick Bontis. 2007. User acceptance of wireless short messaging services: Deconstructing perceived value. *Inf. Manag.* 44, 1 (2007), 63–73. DOI: https://doi.org/10.1016/j.im.2006.10.005

[53] Ofir Turel and Yi (Jenny) Zhang. 2011. Should I e-collaborate with this group? A multilevel model of usage intentions. *Inf. Manag.* 48, 1 (January 2011), 62–68. DOI: https://doi.org/10.1016/j.im.2010.12.004

[54] Viswanath Venkatesh. 2000. Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Inf. Syst. Res.* 11, 4 (December 2000), 342–365. DOI: https://doi.org/10.1287/isre.11.4.342.11872

[55] Hui-Ju Wang and Jin Lo. 2016. Adoption of open government data among government agencies. *Gov. Inf. Q.* 33, 1 (January 2016), 80–88. DOI: https://doi.org/10.1016/j.giq.2015.11.004

[56] Vishanth Weerakkody, Zahir Irani, Kawal Kapoor, Uthayasankar Sivarajah, and Yogesh K. Dwivedi. 2017. Open data and its usability: an empirical view from the citizen's perspective. *Inf. Syst. Front.* 19, 2 (April 2017), 285–300. DOI: https://doi.org/10.1007/s10796-016-9679-1

[57] Wei T. Yue, Qiu-Hong Wang, and Kai-Lung Hui. 2019. See no evil, hear no evil? Dissecting the impact of online hacker forums. *MIS Q.* 43, 1 (January 2019), 73–95. DOI: https://doi.org/10.25300/MISQ/2019/13042

[58] Raymond F. Zammuto, Terri L. Griffith, Ann Majchrzak, Deborah J. Dougherty, and Samer Faraj. 2007. Information technology and the changing fabric of organization. *Organ. Sci.* 18, 5 (October 2007), 749–762. DOI: https://doi.org/10.1287/orsc.1070.0307

[59] Valarie A. Zeithaml. 1988. Consumer perceptions of price, quality, and value: A means-end model and synthesis of evidence. *J. Mark.* 52, 3 (July 1988), 2. DOI: https://doi.org/10.2307/1251446

[60] Anneke Zuiderwijk, Marijn Janssen, and Yogesh K. Dwivedi. 2015. Acceptance and use predictors of open data technologies: Drawing upon the unified theory of acceptance and use of technology. *Gov. Inf. Q.* 32, 4 (October 2015), 429–440. DOI: https://doi.org/10.1016/j.giq.2015.09.005

Received December 2020; revised February 2021; accepted April 2021