https://doi.org/10.48009/2_iis_2019_172-182

Issues in Information Systems
Volume 20, Issue 2, pp. 172-182, 2019

PRIVACY AND SECURITY TRIBULATIONS IN THE DIGITAL CULTURE

S.C. Spangler, Middle Georgia State University, scott.spangler@mga.edu

ABSTRACT

The ethnographic research project profiles a Southwestern Pennsylvania university's digital culture to understand cybersecurity and device protection literacy. This research will attempt to understand if the higher education digital culture shares the same meanings and associations with social media and communication technologies as the past literature demonstrates. To frame the IRB approved ethnographic observation (n=23), the researcher will utilize Boyd's (2014) four constructs: persistence, visibility, spreadability, and searchability. The findings conclude similarities in the higher education digital domain to the K-12 culture. The results also conclude the possibility of more significant naïve actions towards security and technology privacy negligence.

Keywords: Social media, privacy, privacy and security on the internet, risk, and risk perception

INTRODUCTION

Turkle's (2011) research smeared society as anti-social. The scholar cited digital innovations like the smartphones as the agent causing a face-to-face communication failure. Over the past 18 years, digital students have been considered sophisticated, multitasking individuals with world views and openness. Prensky's (2001) formative research launches a framework to understand who is a digital native and what is a digital culture. Additionally, the study defines a gap in technology acceptance and Internet savvy individuals.

Dana Boyd's (2014) research observes a youth society connected and filled with virtual space, which was first reflective in Palfrey & Gasser's (2010) findings. Boyd's review extensively covers American high school aged digital students. The research explored how the participants find intuitive methods to navigate around authority through social devices and technologies. It also demonstrates a culture filled with vibrant social gatherings in cyberspace.

Unfortunately, the researcher's findings point out the culture having a naïve association towards protection and privacy. This discovery is mainly observed when the youth interact with social media domains and having limited authority monitoring. But more importantly, Boyd's (2014) research portrays a cultural shift, "As social media becomes increasingly ubiquitous, the physical and digital will be permanently entangled and blurry. Innovations will introduce new challenges, as people try to reimagine privacy, assert their sense of identity, and renegotiate everyday social dynamics" (p. 211).

This paper will attempt to filter out misconceptions and understand complimentary findings of the digital culture as they have progressed into the higher education domain since Boyd's (2014) research. Notably, this research will attempt to understand if the higher education digital culture shares the same meanings with technology, social media, and communication as the past literature shares. To construct the view, it will utilize Boyd's four frames of discovery: persistence, visibility, spreadability, and searchability.

Literature Methodology

Galileo Virtual Library search engine is used to construct the literature body. The literature review considers peer-reviewed, full-text journal publications in four scholarly domains: Computer Science, Technology, Communications & Mass Media, and Social Sciences and Humanities. The researcher uses two sets of five keyword search queries: Social media, privacy, privacy and security on the Internet, risk, and risk perception. The second query posted the additional term: digital natives. The query acquired 51 scholarly texts and books for review on the query. However, the researcher excludes incomplete publications, abstracts, or publications stretching outside of the social media scope or mobile technologies consideration.

LITERATURE REVIEW

Chen & Kim, (2013) sought to understand privacy concerns and misuse of Internet social networks. The survey utilized 1044 university students in a snowball sampling construction from two colleges. The researchers' hypothesis suggests the user's gratifications directly correlated with privacy concerns and problematic social networking edifices. Six factors were found as influencers in gratifications: virtual community, diversion, self-preservation, relationship maintenance, relationship building, and information seeking. The researchers discovered two factors for predicting problematic social networking risks: self-presentation and relationship building. The scholars note respondents fail to recognize privacy risks with "unauthorized access, errors, and the collection did not play significant roles in constraining their compulsive, problematic, SNS [social networking site] use" and behaviors (p. 809). Comparably, Quinn's (2014) findings correlated the for-profit nature of social media sites and sponsorship lead participant users away from the ability to normalize behavior. The vendor and third-party domains in social media sites fold security dynamics and layers into multiple underscored activities in which an average users' actions are insignificant for protection. To understand the problematic nature of social media sites, Breaux, Hibshi, & Rao, (2014) examination of developer practices in social sites required a modicum of "tier" evaluations. The researchers suggest users view security and privacy "holistically" and fail to understand the depths incorporated with security on social media sites. This distracted user view, allows developers to easily incorporate deceptive actions.

Similarly, Yu, Hu, & Cheng, (2015) survey of 500 university students find students fail to recognize how radially they self-disclosure information on social media sites. Interestingly, scholars link privacy risks directly to users' social media practices to increase relationships. Additionally, the researchers used the intensity model test to determine users' behavior. The findings suggest high-intensity levels have indirect effects on self-disclosure. Notably, the scholars discover high-intensity users of social networks increase behavior risks directly (p. 257). Overall, the dangers of negative self-disclosure actions outweigh users' motivators.

Steijn & Vedder's (2015) Netherland survey of 1002 participants (12 to 83-year-old citizens), observed users' considerations about privacy and releasing personal information on social networking sites. The scholars create a privacy reduction scale that explains how age determines and demonstrates higher privacy risk considerations. Interestingly, the researchers observe females considering "privacy and security more essential" than males (p. 305). Overall, Steijn & Vedder's (2015) viewed autonomy (age nondiscriminant), positively relates to privacy importance. Similarly, Whitty, Doodson, Creese, & Hodges's (2015) survey of 630 UK professionals shows 62% limit privacy through sharing passwords explicitly. And the scholars suggest the younger users are on devices, the more likely they are to have no modicum of self-monitoring and locus of control. The scholars found three predictors for showing a lack of privacy while on social media sites: age, perseverance, and self-monitoring.
Conversely, Hua Dai & Yan Chen, (2015) posits social exchanges are merited not on age or perseverance, but through a user's perceived value of a site. The scholars point out users have a more significant loss of monitoring while utilizing mobile devices, especially while transmitting data on social and commerce domains. Nevertheless, the scholars contradict themselves stating users increase their privacy risks for social exchange benefits. These regards follow Chen & Chen's (2015) findings on 559 university students that determined a significant correlation between self-efficacy in privacy management and privacy-protecting behaviors. Notably, the research observed users' friending behaviors on social media sites positively correlates to the amount of loss in security and privacy.

Autonomy and Social Sites
Pool's (2013) examination recognized the "revolutionary impact" on an individual's data while using social media. Interestingly, the researcher discovers users have a fraction of privacy expectations, and they don't understand the unconstrained digital borders of social media. The scholar suggests user's privacy controls are "limited" and unprotected through states' laws, which are riddled with ambiguity (pp. 413-414). Users are prone to accept risks because of the ease of use and flexibility of social sites.
Similarly, Jiwa et al., (2013) participants find social media sites reduce "economic burden." Participants are willing to accept risks in social site use when it reduces an economic burden. Notably, risk acceptance is greater when users foresee a perceived benefit in social media use. Participants' financial burden was identified as a key "impetus" to accept social media risk factors, particularly on mobile technologies. This risk also prohibits an individual's ability to hide their information or identity.

Faresi, Alazzawe, & Alazzawe's (2014) research considers autonomy and pseudonyms influence on privacy in social media sites. The researchers' tests demonstrate how pseudonym profiles could influence users' identification and practices. The researchers' participant sample (n=243), all utilizing pseudonym profiles, were all identified through social engineering and ethical hacking methods. The pseudonym identities left users subject to privacy and security losses. The researchers demonstrate although pseudo profiles utilize, 41% of users are identifiable through sensitivity mapping alone that includes first name regeneration, age, image matching, and other values (pp. 529-533). Similar to the findings of Pool (2013), Faresi, Alazzawe, & Alazzawe's (2014) suggest users are limited in privacy protocol protections and understanding of their protections' limitations.

Digital Culture Literature Review

Researcher Don Tapscott first discusses digital pen pal relationships in early 1992. His scholarly study leads to two decades of Internet research affects. Tapscott's (1999) technology-based "friending" coined the initial Net Generation paradox. The initial research stems from a survey population of 300 "youngsters" aged four to 20-year-olds on a virtual forum called Growing Up Digital. The original research coins the community as "hungry for expression, discovery, and their self-development." It also labels the youth as having "accelerated child development… social skills… including cognitive intelligence, reasoning, personality, and, through, adolescence, the creation of autonomy, a sense of the self and values" (Tapscott, 1999, pp. 4-7). With the new Internet culture evolving, Tapscott's (1999) digital forum precludes culture "disturbances" rising and the need for "Netiquette." Particularly, Tapscott's foresight observes a need for a discussion on ethics and identity respecting, which he calls the privilege of silence, fair treatment, and anonymous authentication (pp. 67-75).

Tapscott's (1999) authentication and trust conditions prematurely explore Internet privacy. The scholar views negative privacy concerns as youthful naïveness. Bauerlein's (2007) survey population cited a generation rife in incompetence with an underlying lack in understanding of digital security, privacy, and technologies mechanics. The scholar describes the digital native culture as having a multitasking ethos that is unsophisticated, riddled with concentration issues, and lacks judgment with privacy and security issues on the Internet. Overall, Bauerlein claims the digital native culture is the "dumbest" generation. The unconventional cultural coining or paradoxical shift suggests a need for education in privacy and security knowledge.

Howe & Strauss' (2000), who somewhat contrasts Bauerlein's view, first explores the social activist nature of the Net Generation. The scholars explain digital empowerment through "fiber-optic cable" friendships are changing the shape of communication and culture (p. 310). The Virginia based survey of 660 high school seniors and 200 teachers explored the roots of Internet social exchanges and group "mobilization." It points out how Internet groupings foster learning and a method for social change specifically in cases of child-sex exploration, child labor bondage, and information privacy (p. 302). Materialistically, Howe & Strauss' (2000) explores the transgression of public intimacy and a growing generational naiveté similar to Palfrey & Gasser's (2010) study. Palfrey & Gasser's research explores the culture earlier and describes it as rife with individuals not protecting the privacy and personal information. Both sets of scholars recognized the immediate danger of individuals not protecting their "medical, academic histories, credit-card information, online banking transactions and security cameras that capture the comings and goings" (Palfrey & Gasser, 2010, pp. 54-55). More pointedly, Palfrey & Gasser's research cited individual security awareness fallacies. Palfrey & Gasser's survey population explores how the culture lacks education privacy and security and good practices with the Internet and social media considerations. Pointedly, the researcher's focus groups on 100 "young individuals" shadows a "no guilt" behavior culture and a very complex online society steadily increasing with complex dangers, which includes cyberbullying stalking. Palfrey & Gasser's research cited a 77% cyberbullying increase from 2005 and an increase in cyber identity fraud, stalking, and or predatory complications (pp. 92-99). Since this research started, other scholars are uncovering alarming increases and new areas of privacy and security problems.

Boyd's (2014) research frames a social media or "networked public spaces" problem through four domains: persistence, visibility, spreadability, and searchability (p. 11). Boyd defines persistence as the "durability of online expressions and content" in connection with digitally mediated environments (p. 11). Persistence is the implications of social media actions are not "empheral" but are indefinite and transferable. Further, the scholar explains the privacy of social media exchanges are limitless in spreadability, searchability, time, distance, and transference degree. Boyd describes social media messages as transferable (spreadable) and durable (searchable) over time rather than pastoral transmissions of person to person that are less tangible and indefinite.

Additionally, Boyd describes the new k-12 culture as problematic and tethering to mobile devices. Correctly, Boyd points out that the culture is utilizing social media for connectivity and creating meaningful friendships for "advice, support, entertainment, and a connection that combats loneliness" (Boyd, 2014, p. 17). Interestingly, researchers are discovering digital natives' security and privacy protocols are diminishing or being forgotten because of the increasingly ubiquitous nature of devices particularly mobile devices used for social media purposes. The mobile ecosystem increases the vulnerability of digital natives' naïve nature and scholars have observed it lessens their sensitivity to protect information. Additionally, because of greater reliance on mobile and interactive innovations (smartphones), users are negligent or haphazard in updating and using security protocols. This leaves the users' devices at a greater risk for penetration. The finding further shadows the digital native's culture having a lack in judgement on privacy-preserving measures Kambourakis, Marmol & Wang (2018). Similarly found, Kirschner and De Bruyckere's (2017) academic interpretation of digital natives observes students labelled digital natives are automatically ascribed abilities. The scholars contend the literature's assessment of the culture's ability to multitask and process information through devices is incorrectly assessed. The researcher's present constructs and evidence portraying the culture as lacking in information multitasking abilities and innovation protocol awareness. Furthering the assessment, academics have concluded that digital students are lacking cybersecurity education and 60% of surveyed students in Ndiege & Okell's (2018) survey uncovered they have never received any information security training. Other scholars cite the culture's obsession with unsecured networks connectivity behavior as the attribution to increased vulnerability (Gkioulos, Wangen, & Katsikas, 2017, pp. 2-3). Furthermore, research state the new "smart" technologies and innovations have lessened the digital native's attentiveness or consideration towards privacy and security protocols (Kamber, 2017, p. 3). Privacy consideration is directly correlated with users' sophistication and knowledge of device (security) protocols. Scholars contend education towards instituting the protocols and updates regularly are key factors in protecting youth's privacy and security (Ophoff & Robinson, 2014; Gkioulos et al., 2017; Wang and Xing, 2018). Overall, academic researchers studying the higher education domain conclude a strong need for universities and colleges to create information literacy and information security training protocols in curriculum. Again, Boyd's (2014) reflections uncovered a considerable amount of new privacy and security issues in the k-12 digital culture. Interestingly, the literature's focus on K-12 students creates a significant gap in research.

Statement of Problem

Social media and social applications are a new virtual frontier lacking control and privacy. Digital education on security, privacy, and self-monitoring practices are limited today in society. Past literature studies have focused on the K-12 student body creating a gap in knowledge about higher education students needs for education and practices in the cyber domain. With the gap in the literature's body, the researcher first finds a need to question whether the negatively associated problems with past social media and technology practices are still in repetition?

Statement of Purpose

The purpose of this research is to understand if the new higher education digital culture has been educated about the adverse effects of social media usage and privacy lose through unprotected device usage? Notably, the researcher will explore if Boyd's (2014) four domains: persistence, visibility, spreadability, and searchability are still commonly misunderstood and causing the privacy and security issues in the culture? The research will directly investigate and question the culture's understanding of the Internet and technology privacy. Additionally, the study will attempt to disclose any misconceptions about the digital culture's perceptions of social media persistence, visibility, spreadability, and searchability. For the purpose of this paper, Boyd's (2014) definitions of the four domains will be attributed:

1. Persistence: the durability of online expression and content;
2. Visibility: the potential audience who can bear witness;
3. Spreadability: the ease with wich content can be shared; and
4. Searchability the ability to find content. (p. 11)

METHODOLOGY

The ethnographic research is approved by the California University of Pennsylvania's Institutional Review Board and Robert Morris University's Institutional Review Board. The research design consists of an ethnographic observation in a common area (social area) on the California University of Pennsylvania Campus over one year. The ethnographer posted signs in social domains stating, "Ethnographic observation is being conducted in this area" and disclosed to all participants that research is being conducted. Any persons not willing to participate in the study have been eliminated from the observations and comments.

To understand the data, the ethnographer shadows Spradley's (1980) participant observation techniques. Additionally, to describe the ethnographic rostrum, the researcher frames the observations through Goffman's (1986) stage analysis concept. The methodology allows the researcher to paint and record meanings in the domains for the readers. To triangulate the data, the researcher utilizes Spradley's in-member informants' checking method. Additionally, the researcher utilizes a new concept of ethnographic informant focus group authenticating to triangulate the data's construction and authenticity.

Additionally, artifacts (social media posts or text data) were further shared with informants to validate meanings and actions. The researcher uses the informants' views to shed deeper insights and clarity specifically into Boyd's (2014) associations: persistence, visibility, spreadability, and searchability. Additionally, to foster deeper meaning and understandings of the actions, the researcher conducted a structured participant focus groups to validate the group's thoughts on the data's construction and findings authenticity. The focus groups contained direct informants to assert discoveries' factuality and validity. To create this research domain, the ethnographer bends from traditional ethnographic agile techniques to create a newly coined fluid embedded ethnography methodology.

Fluid embedded ethnography roots its directions and observation methodology in agile ethnography concepts. In an agile ethnography, the researcher utilizes interactive practices rooted in the anthropological participant-observation methodology but bounded within the workplace or business culture. The inductive-adaptable is flexible, "short-term, fast-paced research process" is designed to explore and capture the social-cultural environments and communication and information systems inside a business culture (Borkovich & Skovira, 2018, p. 46). In this research, the new methodology focuses on the 18-23-year-old social culture–whereby digital innovations are utilized particularly for communication, socialization, and gaming. Here the population subgroup consisted of 18-24-year-old higher education male and female students enrolled in traditional university setting and hybrid courses. To further understand social culture, the researcher ascribed its meaning to a location (a facility such as a library, gym, auditorium, or in this case a commuter student common area). Here users can easily engage freely in expression, communication, and gamming through face-to-face interactions and WiFi enabled devices such as laptop computers, iPads, or Smartphones.

In the fluid embedded ethnography observation methodology, the researcher is conscious and aware of the culture prior to entering the domain and able to observe, collect data, and form theories through an embedded technique. The embedded technique is driven from the journalistic embedded war photographers and writers' approach. The fluid embedded ethnographer captures information and data from a cinematic (stage) participant-observer methodology reflective of Goffman's (1986) scientific conceptualization. The concept of embedded persons is not exclusive journalism but assimilated often in academia. The embedded terminology arises from the war correspondents (reporters) being permitted to entrench themselves in combat zones with troops for fast action reporting and in-depth slices of life and activities in a culture (Kesselman & Watstein, 2009). Whereby in this case, the researcher becomes a constant collaborator that can easily assimilate into the culture and befriend the individuals under investigation. This action is similar to the academia's embedded librarian roles in face-to-face, hybrid, and virtual spaces to expand library services (Dewey, 2004, p. 5). To create the ease of the embedding process, the fluid ethnographer utilizes his "known" acquaintances to gain embedment in a small dichotomy of the larger culture under study. The befriending embedding action allows the researcher rich access and immediate acceptance in the culture. In most cases, like the embedded journalist actions, the culture is a subgroup (small culture) inside of a much larger culture being studied.

Additionally, to create validation of the data, the fluid embedded ethnographer will utilize the phenomenological and grounded theory methodologies. This process uses participants as mini focus groups. The in-member focus groups

allow the researcher through in-member checking of uncovered artifacts and a data to validate and triangulate meanings. The non-traditional ethnographic concept allows the researcher to generate deeper meanings about uncovered artifacts and data from the emic perspective with cross-cultural validation. The befriending embedded action allows the researcher rich access and immediate validation to data's constructs without creating misinformation or biases. The fluid in-member focus group validation action allows the researcher to validate the views and observations in real-time voices, meanings, thoughts, or fluid interpretations from, multiple in-members. The real-time focus group assessment creates a deeper meaning behind interpretations and validations to the findings. Additionally, the focus group validations allow the researcher to generalize the findings to the larger population under examination similar to a war correspondent's ability to prescribed overall troop attitudes based on a small embedded culture's views. In this fluid embedded ethnography, the artifacts, data, and findings are similarly validated and constructed to form an opinion of the larger population and student body under examination.

In this research case, the ethnographer inserts himself in a small (similar to the war correspondents entrenching in a small tank brigade in warfare areas such as the Gulf War) population in the social area (commuter gaming and rest area on campus). The embedded researcher's presence fluctuated according to time and location the small population congregated daily. The small forum of in-members varied from a low of 23 to a high of 53 individuals. This fluctuation is similar to warfare movements of small recon troops in a battle zones ebbing and flowing for information gathering and reconnaissance. Similar to the agile methodology, informants were not disclosed to other participants to provide a biased opinion. The informant protection offered a third-level of triangulation to add profound clarity and meanings to the observations. The informants–who are undisclosed and protected–provided deep associations into the actions of their peer participants with an emic perspective.

For this paper, the researcher will examine one domain (culture) with multiple informants clarifying artifacts for validation from the embedded perspective. The area under investigation associates two spheres: online and in person. The field of study demonstrates a rich data capturing arena. The data capture occurs through multiple actions: a series of social media messenger exchanges, mobile device transmissions (text messages), and subsequent social-media site pages. The sphere consisted of a social media sphere (Facebook), and an analog gaming location located in Herron Hall composed of 23 participants and informants. The researcher participates indirectly (virtually) and in person in the social sphere as an embedded fluid ethnographer announced to the culture. Key male and female informants permit the researcher to monitor virtual exchanges on Facebook and its virtual messenger platforms (observed on mobile smartphones) during the ethnography. The overall findings are generalized to the larger population of 500 18-23-year-old male and female higher education students being observed in the master ethnographic study. The overall study lasted one year from May, 2014 to May, 2015.

RESULTS AND DISCUSSION

Discussion of Boyd's (2014) Constraints

Boyd (2014) defines persistence as the "durability of online expressions and content" (p. 11). The ethnographic observation first concurs with Boyd's data in the persistence area. Additionally, it uncovers new data and artifacts in connection to persistence. Notably, the ethnographer observes a culture filled with privacy negligence and privacy avoidance. In the research sphere, social media (Facebook) constructs a conduit for social gatherings in many existences: face-to-face, internal university domains, and global instances. The social media (Facebook) platform forms a mere method to communicate at the level of a virtual bulletin board. The innovations such as smartphones constructed the conduit into the social forums, and a means to communicate needs for face-to-face gathering sites. Interestingly found, each social gathering formed deeper meanings and cultural constructions: gender, race, and social status breakdowns.

The cyber gatherings are a conduit for constructing person-to-person activities in the culture and not a fluid exchange system of information. Additionally, the research found the information the students' post is not moderated or verified for accuracy. As an example, digital students utilized social media blasts on Facebook to organize gaming activities (card games) on campus in the face-to-face realm. The conduit (Facebook) linked participants to time, space, and duration to muster. The call to action in the Facebook sites was nothing more than an urge to assemble and play a card

game called Magic: The Gathering. The call to organize was observed in Boyd's (2014) research as a sophisticated way in which "technology interacts with society" (p. 212).

The cyber call to assemble postings on Facebook coincided with Boyd's findings of privacy negligence and vulnerability. As an example, the cyber (Facebook) announcements left participants vulnerable to privacy constraints, which led to public mocking and ridicule by third-party witnesses online and in person. In most cases, the third-party actors were part of the Facebook group (outsiders) but left out of the face-to-face gatherings. Informants disclosed, during the analog gaming session, outsiders use the group's social media and mobile technologies for deceptive practices. Mainly, the outsiders utilize the group's Facebook channel and instant messenger feature to share private exchanges (hidden from the entire groups viewing) with both negative and positive actions. This action uncovers in Boyd's (2014) research on K-12 digital natives.

Spreadability

Boyd's (2014) research uncovered K-12 digital natives' methods to spread messages. Boyd describes this as the "ease" content cane be shared (p. 11). Similarly, this research revealed Facebook messenger as a core method to exchange hidden messages from all group members without considerable technological skills. The exchanges were person-to-person and used for internal hidden messages. Notably, the actions and artifacts revealed deceptive practices. The social exchanges between informants mocked group members for social graces during the Card Game. (Virtual transactions were conducted between participants through mobile devices underneath the gaming table. Participants used the Facebook messenger tool and text messages to exchange criticisms and not positive social exchanges). The Facebook messenger exchanges became taunting exchanges. Group participants became "hurt and shamed" once the privacy of the messaging uncovered by the researcher's key informant and disclosed to unwanted recipients. The Facebook messages created a feeling of shame inside the face-to-face group. This concept reflects Boyd's (2104) observations stating spreadability of virtual messaging and privacy is misunderstood in the K-12 Culture.

Spreadability Positive in Intention

Spreadability is considered the "ease with which content can be shared" through digital social networks (Boyd, 2014, p. 11). Spreadability connects privacy and persistence through the actions of self-expression. Although the core of the messages is deceptions, informants demonstrate positive social exchanges too. As an example, two female participants' exchanges and artifacts–although deceptive–were earmarked positive in intention. While male participants engaged in the analog card game in the sphere, the female members' text message exchanges through Facebook to discuss communication skills and relationship questions. The point-to-point virtual messaging by the females were somewhat deceptive but in actuality were positive practices. The transactions were protected communications about desires and passions to date male counterparts. Ironically, the male participant of desire by the females was similarly and virtually at the same space and time exchanging equal virtual considerations. The considerations–virtual testaments of love or dating desires–remain controlled and private as long as actors devices were physically protected and locked for privacy. The uncovered artifacts represent a change in the digital native culture about the need to protect private exchanges. This was uncovered in Boyd's (2014) research but pointedly in the deceptive communication forms only. The demonstration by the two counter sexes in the higher education domain illustrates a knowledge of privacy and methods to secure data privacy through social media applications.

Visibility

Boyd's visibility concept frames how participants demonstrated ill regards towards artifact privacy. As an example, a female participant's mobile device (left unguarded and not password protected), posted a private message on the device's screen. Boyd's (2014) visibility labels this cyber security impropriety as "potential" to "bear witness" (p. 11). The equipment left unguarded, disclosed the private message and a series of private social media exchanges. A male participant discovered the notes on a females' unguarded device. Boyd's visibility context frames the third-party or externalities with social media audiences. Boyd describes visibility as "the potential audience who can bear witness" to social media users' actions. Visibility questions privacy through a direct connection of second party recipients and with limited associations or regards towards third-party actors. In the case of study, the fundamental disclosure of virtual messages demonstrates how third-party participants receive protected private social messages.

Searchablity
Boyd's (2014) searchability context parallels visibility action. Searchability is defined in the context of the ability of an external user or non-community member to "find content" (p. 11). Searchability connects users' privacy and actions with visibility but in connection with third-party actors receiving messages or artifacts deceptively. The researcher's data confirm Boyd's searchability aspects. Informants disclose in the ethnography how they could follow females on their Facebook site and their collapses through simple community reposts. (A Facebook collapse occurs when in-members repost another's artifact without security constraints attached). The searchability of collapses allowed male members to breach privacy considerations and find information thought to be private. When an in-member post on an open collapse conversation, anyone inside the or connected to the user can view the searchable public conversation. In this ethnography, females posted statements in collapses that were not protected. The collapses breach females' privacy because they lacked security in social media protocols. Hence, the repeated public collapses in the group opened the originator to searchability characteristics. The content, which was inappropriate, signaled similarities to Boyd's (2014) "ephemeral gestures" the K-12 digital natives used with Snapchat viewing. Although, the spreadability, in this case, has a positive effect.

Additionally, in the Facebook collapses, emic members shared valuable information such as cards for sale, dates and times of next social gathering, and knowledge of others interested in joining the group. This can be viewed as a positive association with searchability. Although, the same fold entertained negative associations through public openness in the postings. As an example, virtual non-members folded responses to the groups' public (semi-private virtual) posting. The group observed face-to-face mockery from the outside non-members witnessing the posting. The virtual bullies appeared in person at the social event in a semi-non-threating measure (a few outer group members came to the face-to-face sphere and taunted members). Although the action was non-violent, informants confessed the taunting did cause trust issues with spreading information again virtually. Boyd's visibility context frames the third-party or externalities with social media audiences. Boyd describes visibility as "the potential audience who can bear witness" to social media users' actions. Virtual trust and privacy are considered easier to void or breach. In the social media environment, verification of identity and recipient becomes "asymmetric, and users do not trust each other in the same way… and trust evolves over time" (Paliszkiewicz & Koohang, 2016, pp. 74–75). Visibility questions privacy through a direct connection of second party recipients. In the case of study, the fundamental disclosure of virtual messages demonstrates how third-party participants can receive private social messages.

Additionally, the deviant spreading of the females' virtual messages about love interests caused cognitive hardships. The girls–at first–consider the actions (theft of virtual notes), damaging of interpersonal trust and more importantly privacy. The breaks in trust/privacy formed barriers not demonstrated prior. The spreadability of privacy barriers surpassed the female members and circumnavigated the group. The restrictions were witnessed through members pocketing and hiding devices, changing passwords, and overall physical sheltering of body and openness. The actions (artifacts) demonstrates a cognitive representation of privacy invasion and limitations in trust mechanics. Despite the privacy barriers, member informants overcame the privacy breach quickly. The action at first was considered negatively but changed quickly once a male member confessed excitement at receiving the hidden message. The female informants disclosed that the virtual theft of private exchanges first caused fear, anxiety, and trust issues. Although, once the male's confession occurred, the informants disclose excitement and reduced stress from the disclosures. This finding of privacy and trust also parallels Boyd's (2014) consideration. It shadows the K-12's social steganography practices to encode messages that are in public views.

CONCLUSION

Boyd's (2014) research frames a social media or "networked public spaces" problem through four domains: persistence, visibility, spreadability, and searchability (p. 11). Throughout this fluid ethnographic investigation, the research uncovered artifacts of similarity in each area. Informants' disclosures confirmed the artifact observations and described the culture having no less or no more complication with social media and privacy as the K-12 generation. It, however, does appoint a greater measure of cyber security impropriety especially observed in the visibility and spreadability domains in Boyd's (2014) research contemplations. The research uncovered similar difficulties with Facebook privacy, use, and connectivity. It also found parallel privacy conflicts with other social media platforms like

Snapchat. Notably, it revealed a culture misunderstanding the spreadability and searchability with social media posts and conversations.

Further, the research uncovers a more negligent knowledge about the privacy on social media and the higher education culture misunderstanding its limitlessness in time, distance, and transference degree. Additionally, the research concurs with Boyd's descriptions of problematic digital tethering to mobile devices for connectivity. Although this may be considered harmful, the actions create a positive mechanic. Here in this research it again shadows Boyd's findings. The practice demonstrates a method to create meaningful friendships for "advice, support, entertainment, and a connection that combats loneliness" (Boyd, 2014, p. 17). The researcher's ethnographic investigations confirm Boyd's virtual friendships and how the culture uses technology to elevate "awkward" traditional face-to-face conversation through social media and smart devices.
To further the research, the scholar suggests comparing a large population as Boyd's (2014) study was able to construct. The researcher acknowledges the small community and focused observation area was located in a socio-economically deprived area. The downturned socio-economic area may have caused a limitation for participant access to new or more popular smart devices. Additionally, the researcher suggests the need for a comparison study between European countries and the United States to understand if similar constructs are only observed in this culture.

REFERENCES

Bauerlein, M. (2007). Dumbest generation. Retrieved June 5, 2014, from http://www.dumbestgeneration.com/home.html

Borkovich, D. J. & Skovira, R. J. (2018). Agile ethnography: Interpreting organizational cultures in the informationage. *Journal of Ethnographic & Qualitative Research*, *13*, 46-61.

Breaux, T., Hibshi, H., & Rao, A. (2014). Eddy, a formal language for specifying and analyzing

data flow specifications for conflicting privacy requirements. *Requirements Engineering*, *19*(3), 281–307. https://doi.org/10.1007/s00766-013-0190-7

Byod, D. (2014). It's complicated: The social lives of networked teens. New Haven, Connecticut: Yale University Press.

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and

self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior and Social Networking*, *18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Chen, H.-T., & Kim, Y. (2013). Problematic use of social network sites: the interactive

relationship between gratifications sought and privacy concerns. *Cyberpsychology, Behavior And Social Networking*, *16*(11), 806–812. https://doi.org/10.1089/cyber.2011.0608

Dewey, B. I. (2004). The embedded librarian: Strategic campus collaboration. *ResourceSharing and Information Networks*, *17*(1), 5–17. https://doi.org/10.1300/J121v17n01_02

Faresi, A. A., Alazzawe, A., & Alazzawe, A. (2014). Privacy leakage in health social networks. *Computational Intelligence*, *30*(3), 514–534. https://doi.org/10.1111/coin.12005

Gkioulos, v., Wangen, G., & Katsikas, S.K. (2017). User modelling validation over the security awareness of digital natives. *Future Internet*, 9(3), 32. http://doi.org/10.3390/fi9030032.

Goffman, E. (1986). *Frame Analysis: An essay on the organization of experience*. Northeastern.

Howe, N., & Strauss, W. (1993). *13th gen: abort, retry, ignore, fail?* New York: Vintage Books.

Howe, N., & Strauss, W. (2000). *Millennials rising: the next great generation /by Neil Howe and*

Bill Strauss; cartoons by R.J. Matson. New York: Vintage Books.

Hua Dai, & Yan Chen. (2015). Effects of exchange benefits, security concerns and situational

privacy concerns on mobile commerce adoption. *Journal of International Technology & Information Management*, *24*(3), 41–56.

Jiwa, M., McManus, A., Dadich, A., White, J., Rieck, A., & Razmi, S. (2013). Harnessinginformation technology to innovate in primary care. *Quality in Primary Care*, *21*(1), 43–49.

Kamber, T. (2017). Gen X: The cro-magnon of digital natives. *Generations*, 4(3), 48-54.

Kambourakis, G., Marmol, F. G., & Wang, G. (2018). Security and privacy in wireless and mobile networks. *Future internet* 2018. *10*(2), 18; https://doi.org/10.3390/fi10020018

Kesselman, M. A., & Watstein, S. B. (2009). Creating opportunities: Embedded Librarians. *Journal of Library Administration*, *49*(4), 383–400.

Kirschner, P.A. & De Bruyckere, P. (2017). The myths of digital native and the multitasker. *Teaching and Teacher Education.*, 67(10), 135-142; https://doi.org/10.1016/j.tate.2017.06.001.

Ndiege & Okell's (2018). Towards information security savvy students in institutions of higher learning in Africa: A case of a University in Kenya. IST Africa Week Conference, (May, 2018), Gaborone, Bostswana.

Palfrey, J., & Gasser, U. (2010). *Born Digital: Understanding the first generation of digital natives* (First Trade Paper Edition edition). Basic Books.

Pool, M. M. (2013). Personal health information shared via social networking: The gap between reality and protection. *Journal of Law, Technology & the Internet*, *4*(2), 411–444.

Quinn, K. (2014). An Ecological Approach to Privacy: "Doing" online privacy at midlife. *Journal of Broadcasting & Electronic Media*, *58*(4), 562–580. https://doi.org/10.1080/08838151.2014.966357

Spradley, J. P. (1980). *Participant Observation* (1st ed.). Holt, Rinehart and Winston.

Steijn, W. M. P., & Vedder, A. (2015). Privacy concerns, dead or misunderstood?

The perceptions of privacy amongst the young and old. *Information Polity: The International Journal of Government & Democracy in the Information Age*, *20*(4), 299–311. https://doi.org/10.3233/IP-150374

Tapscott, D. (1999). *Growing up digital: The rise of the net generation* (New edition edition). New York: McGraw-Hill.

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other* (1st ed.). Basic Books.

Wang, X., & Xing, W. (2018) Exploring the influences of parental involvement and socioeconomic status on teen digital citizenship: A path modeling approach. *Journal of Educational Technology & Society*, 2(1), 186-199.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber securitbehaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior And Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

Yu, J., Hu, P. J.-H., & Cheng, T.-H. (2015). Role of affect in self-disclosure on social network websites: A Test of Two Competing Models. *Journal of Management Information Systems*, *32*(2), 239–277. https://doi.org/10.1080/07421222.2015.1063305