Winter 12-13-2018

Ethical Considerations of Online Identities

Atiya Avery
University of Illinois at Chicago

Dream Gomez

Atiya Avery
Department of Information and Decision Sciences, University of Illinois at Chicago,
Chicago, Illinois, United States

Dream Gomez
Atlanta, Georgia, United States

ABSTRACT

In the United States, the personal information of private citizens can end up online many times without permission. This personal information can become publicly available via the internet, where algorithmic driven internet search engines serve as a type of aggregation and retrieval system. Personal information from internet search engines can be compiled and used by frontline practitioners within organizations to form a profile i.e. an online identity about private citizens; where the online identity can be used for making decisions which may cause undue harm. It is not clear if organizations and private citizens are aware of the implications of this phenomenon. This paper discusses emerging concerns regarding the use of internet search engines to form online identities for decision-making and provides an ethical framework in the form of a series of questions to help guide the use of internet search engines and online identities in the day-to-day decision-making processes of frontline practitioners within organizations.

Keywords: Privacy, Identity Management, Ethics, Search Engine, Information Seeking

I. INTRODUCTION

The use of internet search engines as an information retrieval system is a gray area from an ethical, regulatory, and compliance standpoint. Despite this, it is clear that individuals and organizations utilize internet search engines to obtain information on private citizens for safety and verification purposes. Private citizens admitted to utilizing internet search engines to find information about friends and people from their past (Madden & Smith, 2010). A 2013 survey of college admissions officers indicated that 35% of survey respondents were utilizing internet searches on potential students including scouring social media profiles (Schaffer 2013).

In 2015, a survey of 410 human resources professional indicated that 84% of them utilized social media to find job candidates with close to half of those surveyed indicating that they utilized social media as a screening tool of those candidates. 33% of the human resources professionals surveyed indicated that they had not hired a candidate because of information they found online (Ruiz-Elejalde, 2016). However, a 2013 Pew Research Center survey indicated that only 1% of internet users believed that they have lost out on a job or educational opportunity because of information online about them (Rainie et al. 2013). This provides some evidence that private citizens may be grossly underestimating the influences that internet searches and online identities have on the decision-making activities of practitioners and organizations. Not being aware of how internet search engines and online identities are utilized for decision making can potentially lead to negative impacts on the lives of private citizens.

Frontline practitioners use internet search engines to understand an individual's prior behavior to assess their risk levels according to the practitioner or organization's business needs. However, frontline practitioners within organizations who utilize internet searches on private citizens need to understand the risks and benefits of the internet search engine as an information verification tool. Without this understanding, practitioners may inadvertently cause harm. Information found online is missing identity, missing a role definition and may be subject to missing personal characteristics due to the warping of time and space. This missing information requires frontline practitioners who use internet search engines to make inferences about what they find based on their current knowledge, biases, values systems, occupation, geographic origin, and other subjective measures of judgment (Lyon, 2003;Boyd, 2008).

This article discusses the emerging concerns regarding the use of online identities and ethical considerations for the frontline practitioners that utilize these online identities for decision-making. This article is based in part on the moral responsibility framework discussed by Culnan and Williams 2009 and will help to provide guidance for reducing the potential impact of incorrect or misapplied uses of the internet search engine as an information verification tool for private citizens.

This research posits that the responsibility for privacy protections should come from those who will collect and use the personal information of others and that this responsibility is and should be inherently moral in nature. This research seeks to encourage policymakers to consider the broader negative implications when organizations such as financial institutions, universities, and employers engage in the collection and compilation of decontextualized personal information found online.

What follows is a discussion on the evolution of information verification by frontline practitioners using an example of insurance underwriters; this is followed by an overview of the characteristics of search engine data. The paper then discusses how online identities are created in the mind of the information seeker, and finally the paper concludes with a discussion of specific ethical considerations for frontline practitioners when utilizing internet search engines.

II. THE EVOLUTION OF INFORMATION SEEKING AND VERIFICATION FOR PRACTITIONERS

The motivation for frontline practitioners utilizing internet search engines as an information verification tool can be clearly illustrated by understanding the evolution overtime of insurance underwriters but can be applied to other practitioners including admission officers, hiring managers, landlords, and lenders. A fundamental tenet of underwriting is information verification and integrity for risk assessment and assignment (Insurance, 2013; Bhat, 2009). For example, if a driver were purchasing automobile insurance basic questions need to be answered surrounding the drivers age, marital status, and gender. Is an applicant 19 years old or 24 years old? Is the applicant married or unmarried? When applicants are not properly underwritten, financial performance will degrade and the organization can incur losses (Bhat, 2009). Prior to the widespread use of computers, information provided by applicants on paper applications was manually verified. An application for homeowner's insurance simply required a copy of the deed to the home and a visit to the physical location by the insurance agent. The underwriting process has evolved overtime because of improvements in technology (Mckinley, 2010). Furthermore, with the advent of computerized record keeping, organizations have been electronically collecting private information on individuals since the 1960's. Towards the late 1980's and early 1990's technology improved, and computerized records now had the capability to be mined and analyzed (Culnan, 1993). Financial institutions could now achieve greater information integrity by verifying information from the applicants via public databases such as LexisNexis. In 1992, the first patent was filed for a design that connected databases for insurers to verify the current and prior insurance status of a vehicle (Garrett & Tuttle, 1994). Similar types of databases were designed that could validate the accident, claim, and traffic citation history of individuals as well as automobile vehicles through the use of vehicle identification numbers (VINS).

The most dramatic changes in the underwriting process have occurred over the last three decades with the emergence of instantaneous information verification via linked public databases along with algorithmic driven decision support systems which are now utilized to achieve optimal underwriting outcomes (Mckinley, 2010). In 2001, Progressive Insurance Company, one of the largest car insurance companies in the United States, developed one of the first such decision support systems. The decision support system immediately validated information on an electronic application and then used real time data to immediately provide a premium (Henderson, 2001). On the surface, the aforementioned linked public databases and decision support systems are being utilized by organizations to make decisions in what are seemingly standardized and transparent decision-making processes. However, internet searches can also be used to quickly provide additional information to decision makers that public record databases and decision support systems do not. Internet searches are a deviation from the standardized decision-making processes.

Internet search engines allow for the web crawling, indexing, and searching of webpages. They serve as a type of information retrieval system and have become more algorithmic driven (Seymour et al. 2011). Mowshowitz & Kawaguchi 2002, asserted that internet search engines contain organized collections of business records, medical files, and scientific articles that are indexed. Like public record databases and organizational decision support systems, the internet search engine provides a language for asking questions and retrieving the answers.

The use of internet search engines for internet retrieval is being used by decision makers in private and public agencies that have a need for unbiased information or at least knowledge of the bias within their information verification sources. A risk of frontline practitioners utilizing internet search engines for information verification is that many do not understand or consider that this tool, the internet search engines, has built in biases. Search engines are a gauge for political, economic, and social biases in the information they provide (Seymour et al. 2011). It is known that algorithmic driven internet search engines are able to pick up on societal biases towards sex and race (see Noble, 2013; Sweeney, 2013). Biases are a natural part of being human. It is important however, that decision makers are aware and attempt to mitigate against these built in biases when they are utilizing internet search engines on private citizens.

Another risk of utilizing internet search engines especially by organizations is that they may circumvent existing regulations such as the Gramm-Leach-Bliley Act and the Privacy Act. The Gramm-Leach-Bliley Act contains multiple provisions one of which governs the disclosure of nonpublic personal information about consumers by financial institutions. The act requires that customer records be kept secure, confidential, protected against any anticipated threats and from unauthorized access or use. Another important caveat of the provision is that nonpublic personal information not to be disclosed to nonaffiliated third parties without providing the customer notice and the option to opt out (Cuaresma, 2002). However, the use of information obtained from internet search engines seems to relieve organizations of many of these requirements. In addition, the use of internet search engines can then drive the decision makers' use of regulated public databases such as Experian and LexisNexis. In regards to the Privacy Act (includes Fair Information Practices) the use of internet search engines for decision making appears to be at odds with the requirements for purpose, the openness, and the individual participant as well as the accountability specifications (Koontz, 2008) with each specification requiring a specific business reason for wanting to obtain an individual's personal information. Both of these Acts have built in protection allowing the customers to ascertain how information was obtained about them and used in a decision making process. It also gives individuals the opportunity to dispute incorrect information and provide context. The use of internet search engines as an information verification tool does not afford individuals these opportunities and furthermore many organizations are not able to admit that they found information that way.

III. SEARCH ENGINE DATA AND IDENTITY CREATION THROUGH INFORMATION SEEKING

Acquisti, 2008, defines online identity as any information that can be retrieved from the internet about an individual. It is the individuals tastes, thoughts, and purchase behavior. The offline identity refers to the identity of the individual as revealed by social security numbers, credit cards numbers, occupations, and offline social interaction. This paper argues that the boundary between an individual’s online identity and offline identities are blurring due to the prevalence of social networking sites, forums, discussion boards, and online/offline groups such as “meetups” and data breach events. This paper does not make a distinction between online and offline identities and refer to any identifying information online about an individual as part of their online identity.

This paper positions that identifiers of an individual can end up on an internet search engine intentionally or unintentionally through such mechanisms as content creation, data breaches, and app utilization. Table 1 provides examples of intentional search engine data and unintentional search engine data sources. The use of an intentional/unintentional data source classification schema accounts for the phenomena of individuals who do not interact with information technology still having traces of their identifying information and seemingly personal pieces of information available online.

Table 1. Search Engine Data Source Types

Intentional	**Unintentional**
Individual Sharing of the following: News Articles Quotes Music Online Groups membership Writing Blogs Online Discussion Forums Creation of Videos and Music Social Media Newsletters Employer Websites Apps	Third Party Internet Data Aggregators which provide the following: Names Birthdates Property Records Images of Home Public Salary data Arrest Records Foreclosures Other Types of Public Notices

Internet search engines can facilitate the retrieval and compilation of personal and private identifiers allowing practitioners the ability to search for and retrieve personal information about almost anyone at any time. The compilation of identifiers from the internet allows users of internet search engines to form a profile or an online identity about an individual. Personally identifiable information refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linkable to a specific individual (Krishnamurthy & Wills, 2001). Formation of online identities by frontline can also reinforce long-standing social differences (Lyon, 2003). These longstanding social differences may not accurately reflect an identifier of that individual. For example, researchers discovered that internet searches for individuals with traditionally black-sounding names were 25% more likely to imply that the individual had an arrest record in their history (Sweeney, 2013). A prior arrest record is a concern because it forms a negative bias in the mind of the information seeker regardless of whether this history factually exists. This has the potential to impact access to financial products, employment opportunities, schools, and even housing. In addition, information found online can lead to inferences about the individual that they may not wish to disclose or that may simply be incorrect.

Currently, there is no evidence that there are organizational policies, federal acts, or local acts in place to regulate this phenomenon. Hence, self-regulation via an ethical framework is a viable alternative to not only protect organizations but also private citizens. Growths in the uses and capabilities of information technology have caused an increased in the surveillance, communication, computation, storage, and retrieval of personal information (Lyon, 2003). Josang et al. (2005), posits that a characteristic of an individual such as name, address, nationality, group membership, and even biometric information is an "identifier" of a person. Identifiers can be multifaceted but are unique for each person. Through information seeking these identifiers can be linked together to form one or more identities for a person. Individuals who utilize internet search engines engage in a well-defined behavior the extant literature has called "information seeking". Information seeking can be defined as the process of sense making in which a person is forming a personal point of view and is actively involved in finding meaning which aligns with what they already know using a personal frame of reference. A unique aspect of information seeking is that information from various sources is assimilated into what is already known through a series of choices. During the process of information seeking, formal organized sources from information systems interact with informal sources from everyday life experiences. Information from internet searches is not from within a formally organized information system.

One of the drivers of information seeking within organization is to enhance performance. Research has found that organizational information and communication technologies need to not only support information delivery but must facilitate relationship management for the information seeker (Xu et al. 2010). This makes the ease of use of internet search engines attractive. Due to instantaneous information delivery, the volume of information delivered, ease of sharing, and ease of use one can argue that personal, subjective judgements such as life experiences will have more influence on the seeking process i.e. influencing the information seekers unconscious train of thought. Choi et al, 2015, for example found that utilizing internet search engines compared to social media sites for exploratory search tasks people with more diverse, relevant, and larger sets of documents. In addition, study participants reported feeling that the search process was less labor intensive and challenging compared to utilizing social media for exploratory searches. Next, is a discussion of on ethical considerations of utilizing online identities from internet search engines based on the philosophies of 1) vulnerability awareness and 2) harm avoidance.

IV. ETHICAL CONSIDERATION OF ONLINE IDENTITIES: VULNERABILITY AWARENESS AND HARM AVOIDANCE

This section is a presentation of ethical considerations that frontline practitioners within organizations should consider in their day-to-day responsibilities regarding the use of internet search engines in the context of online identities. The concepts of vulnerability awareness and harm avoidance from Culnan and Williams 2009, are the foundation for the ethical considerations as these concepts are at the heart of the moral responsibility framework.

Vulnerability

Vulnerability occurs when one party in a relationship is at a disadvantage in regard to information and control and there essentially exists a power imbalance in the relationship (Culnan & Williams 2009; pg. 679). There is a strong possibility that personal information online can be taken out of its original context and therefore lacks what is called "contextual integrity" (Nissenbaum, 2004; p.101). Information that has contextual integrity is gathered and disseminated to obey the governing norms at the time it was collected (Raynes-Goldie, 2010). There are individuals or organizations with which individuals may be associated but in different contexts. These contexts may conflict with one another. Boyd (2008) elaborates that the internet is full of "network publics", public places on the Internet where different conflicting contexts and social norms coexist. The power lies in the hands of the information seeker to develop the context for the personal information that they find online. This can lead to the information seeker utilizing their inherent biases and assumptions to fill the absence of context especially in the face of little policy or guidance on utilizing the internet search engine as a tool. Leaders of frontline practitioners within organizations need to conduct a cost/benefit analysis to determine if the negative risks of utilizing the internet search engine outweighs the benefits. The following questions should be asked at the onset of an internet search:

> Consideration 1: Why do I feel the need to conduct an internet search on this individual?
> Consideration 2: What is the potential benefit from utilizing an internet search engine tool over approved and traditional organizational information sources in the evaluation of risk?
> Consideration 3: What is the context for the information obtained from the internet search engine?

Mowshowitz & Kawaguchi (2002), observed that internet search engines are an internet retrieval system with organized collections of business records, medical files, and scientific articles that are indexed. The internet search engine provides a language for asking questions and has a retrieval algorithm which is prone to biases. Even in 2002, the research documented that the use of internet search engines for retrieval of information from the internet could be used by decision makers in private and public agencies. Frontline decision makers have a need for unbiased information or at least knowledge of the bias of their sources. To address this, the following set of ethical considerations should be addressed:

> Consideration 4: Would this individual be considered a member of a group in which strong negative social biases exist?
> Consideration 5: Historically, does the practitioner or the organization have pre-existing prejudices about members of this group?
> Consideration 6: Is the practitioner aware of how personal biases would present themselves during an internet search?

The next section is a discussion of ethical considerations related to harm reduction.

Harm Reduction

Harm reduction is based on the notion that organizations and managers within them should not do harm to individuals by mistreating their personal information (Culnan & Williams 2009; pg. 682). Individuals interact with information technology and its artifacts on a daily basis via social media, through self-service software such as human resource management systems and medical care management systems, as well as through the use of apps; disclosing personal information about themselves in the process of these interactions. Individuals may be aware that a trail of their interactions with IT and IT artifacts may be left behind but may assume that only authorized individuals have access to this information or that perhaps information on their interactions is not being used at all. In addition, a defining feature of the internet is the ease in which end users can create and interact with content (Kuksenok et al. 2013). Online content creation is important as it enables communication among an individual's contacts including family and old friends. Internet users who utilize social networking sites such as Facebook, Twitter, Instagram can share pictures, news articles, quotes, music, and even groups that they have joined with their social network allowing others to form views and opinions of them without them having to technically create content on their own. Individuals can also create intimate insights about themselves through the use of personal websites such as blogs, online discussion forums and boards, and the creation of videos and music. In addition, there are a wide range of mobile apps on the market which has access to the individual's internal address book, calendars, and email and social media accounts through the use of single sign on login. Recently, researchers discovered that some apps downloaded from Google Play or the Apple Store are sharing personal information with third parties (Zang et al. 2015). Instagram, which is a very popular photo app, sends users' locations, birthdays, emails, and gender to Facebook.com; whereas Android users of the same app get their identifying information sent to Google. The research also noted that 30% of health and fitness apps were sharing their users medical search terms; with one app reportedly sending medical search term information to Amazon.

In this day and age, it is difficult for individuals to conduct routine activities of daily living without disclosing personal information and it being collected in a digital format regardless of whether or not the individual uses technological artifacts (Culnan & Armstrong, 1999). Personal information in a digital format can easily be copied, transmitted, and integrated with other information (Malhotra et al.2004). There is a misperception that individuals voluntarily disclose their personal information. The disclosure of personal information has become mandatory nowadays even for the most basic of services (Camenisch, et al., 2005). For example, the Chicago Transit Authority requires that both a home address and a billing address be held on file to perform basic online transactions such as adding credit to a transit card. This forces customers who choose not to use cash to disclose this information in order to access public transportation services. A security breach may mean this information ends up online. Public and private organizations of all types have experienced breaches from hospitals, to restaurants, and even voter records have been breach, which contains information such as names, birthdates, addresses, and social security numbers. In 2015, it was thought the data breach of the Office of Personnel Management which involved 22 million federal employee records was to specifically seek individuals in high security clearance roles for intelligence purposes. That same year, the social media site Ashley Madison was hacked leaving 37 million customer records open to public availability and these records were slowly released and lead to two possible suicides (Greene, 2015;Zetter, 2015). The public disclosure of personal information online of private citizen's behaviors and habits has the potential to be a major security issue for organizations of all types.

In addition, personally identifying information found online such as an individual's place of employment, partners, and children can lead to unforeseen consequences. Due to this, individuals have at their disposal strategies to manage their identities (Lampinen et al.2009). Technology savvy individuals may engage in content creation and other measures to fill in the contextual gaps for others so that the information that does appear online about them is trustworthy and accurate. The less technologically savvy are at a disadvantage in this regard and should be protected. Based on these arguments, the following ethical considerations need to be made by frontline practitioners:

> Consideration 7: Would this individual be aware that this information is online about them?
> Consideration 8: Does the individual have the capability to remove or dispute this information from the internet search engine?
> Consideration 9: Could this information have been obtained without the individual's permission or consent e.g. did this information come from a data aggregator or as result of a breach?

Researchers have discovered that consumers who trust the firm that they are doing business with are less concerned about their privacy thus making them more willing to provide the organization personal information during the course of a transaction (Schoenbachler & Gordon, 2002). Furthermore, if a business is trustworthy individuals may be more likely to interact with the business online including using their website and creating content. When individuals trust organizations, they increase the use of services and decrease the privacy concerns that they may have (Hurwitz, 2011). Individuals are concerned about their privacy due to possible issues with spam, identity theft, and fraud (Nam et al. 2006). The literature describes many taxonomies of trust. One type of trust is intentional trust. This describes the end –user's beliefs that a service provider can keep promises regarding security and other issues (Salo & Karajaluoto, 2007). This presents special challenges in the online environment because individuals who create content anonymously or even those who just use information technology and artifacts as apps, and self-service software may be relying on the privacy mechanisms of that service provider. It is important that end users feel that information will not be collected about them that they did not explicitly give permission for as this helps to build and maintain trust. This leads to derivation of ethical consideration 10:

> Consideration 10: Does the organization's privacy policy and/or background check policy specify to the customer that an internet search engine will be used during the background check process?

V. CONCLUSION

Personal information from internet search engines can be compiled and used by frontline practitioners within organizations to form a profile i.e. an online identity about private citizens; where the online identity can be used for decision making. It is not clear if organizations and private citizens are aware of the implications of this phenomenon. However, there are aspects of this practice that without checks and balances may cause undue harm. In countries that are part of the European Union measures are in place for individuals to remove most kinds of personal information from the search engine site google.com. At the time of this writing the United States has no such policies or provisions to govern the protection or proper use of personal information of private citizens gathered from internet search engines. This practice could violate a number of existing consumer protection acts and is not well documented or understood. If frontline practitioners within organizations take moral responsibility for privacy protections this may help organizations minimize the unforeseen consequences of this practice. This paper is intended to bring awareness to this phenomenon and extensive research is needed on this topic to fully document the prevalence and the broader impacts of utilizing online identities in organizational decision-making practices.

REFERENCES

Acquisti, A. (2008). Identity management, privacy, and price discrimination. Retrieved from Self Published

Bhat, A. (2009, August). Underwriting and Risk Management. ISO Review.

Boyd, D. (2008). Taken out of context American teen sociality in networked publics.

Camenisch, J., Shelat, A., Sommer, D., Fischer-Hubner, S., Hansent, M., Leenes, R., et al. (2005). Privacy and Identity Management for Everyone. Proceeding of the 2005 workshop on Digital identity management (pp. 20-27). ACM.

Choi, D., Matni, Z., & Shah, C. (2015). Switching sources: a study of people's exploratory search behavior on social media and the Web. Proceedings of the Association for Information Science and Technology, 52(1), 1-10.

Cuaresma, J. (2002). The Gramm-Leach-Bliley Act. Berkelely, California: Berkeley Technology Law Journal .

Culnan, M. (1993). How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. Management Information Systems Quarterly, 341-360.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. MIS Quarterly, 673-687.

Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 104-115.

Garrett, T., & Tuttle, M. (1994). Patent No. 5,325,291. U.S.

Google. (2017). Remove Information from Google https://support.google.com/websearch/troubleshooter/3111061?hl=en.

Greene, T. (2015). From Ashley Madison to Vtech it has been a nasty breach year . Network World .

Henderson, M. (2001). Patent No. No. EP 1 160 707 A1.

Hurwitz, J. B. (2011). The influence of trust and privacy risk-taking on user acceptance of electronic services that collect personal information. Proceedings of the Human Factos and Ergonomics Society 55th Annual Meeting , (pp. 1110-1114).

Insurance, A. D. (2013). Underwriting and Rating. Retrieved October 25, 2013, from http://www.aldoi.gov/consumers/AutoUnderwriting.aspx

Josang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust requirements in identity management . Proceedings of the 2005 Australasion workshop on Grid computing and e-Resarch-Volume 44 (pp. 99-108). Australian Computer Society Inc.

Koontz, L. (2008). Privacy: Congress should consider alternative for strengthening protection of personally identifiable information. Washington, D.C: United States Government Accountability Office (GAO) .

Krishnamurthy, B., & Wills, C. E. (2009, August). On the leakage of personally identifiable information via online social networks. In Proceedings of the 2nd ACM workshop on Online social networks (pp. 7-12). ACM.

Kuksenok, K., Brooks, M., & Mankoff, J. (2013, April). Accessible online content creation by end users. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 59-68). ACM

Lampinen, A., Tamminen, S., & Oulasvirta, A. (2009). All my people right here, right now: Management of group co-presences on a social networking site. Proceedings of Group , 281-290.

Lyon, D. (Ed.). (2003). Surveillance as social sorting: Privacy, risk, and digital discrimination. Psychology Press.

Madden, M., & Smith, A. (2010). Reputation Management and Social Media. Pew Research Center.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users information privacy concerns (IUIPC) : The construct, the scale, and a casual model . Information Systems Research, 336-355.

Mckinley, E. (2010). Using Analytics to Augment Underwriting. Insurance Networking News.

Mowshowitz, A., & Kawaguchi, A. (2002). Engines assessing bias in search. Information Processing and Management, 141-156.

Nam, C., Song, C., Lee, E., & Park, C. (2006). Consumer's privacy concerns and willingness to provide marketing-related personal information online. Advances in Consumer Research, 212-218.

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(119).

Noble, S. U. (2013). Google Search: Hyper-visibility as a Means of Rendering Black Women and Girls Invisible. Blind Spots, 19.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, Privacy, and Security Online. Pew Research Center.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday, 15(1).

Ruiz-Elejalde, A. (2016, January 11). Using social media to disqualify job candidates is risky. Chicago Tribune.

Salo, J., & Karajaluoto, H. (2007). A conceptual model of trust in the online environment. Online Information Review, 31(5), 604-621.

Schaffer, R. (2013). More college admissions officers checking applicants' digital trails, but most students unconcerned. Kaplan Test Prep.

Schoenbachler, D., & Gordon, G. (2002). Trust and customer willingness to provide information in a database-driven relationship marketing. Journal of Interactive Marketing, 16(3), 2-16.

Seymour, T., Frantsvog, D., & Kumar, S. (2011). History of search engines. International Journal of Management and Information Systems , 47-58.

Sweeney, L. (2013). Discrimination in Online Ad Delivery. latanyasweeney.org.

Weise, E. (2014). 43% of companies had a data breach in the last year. USAToday.

Xu, Y., Kim, H. W., & & Kankanhalli, A. (2010). ask and social information seeking: Whom do we prefer and whom do we approach? Journal of Management Information Systems, 27(3), 211-240.

Zang, J., Dummit, K., Graves, J., Lisker, P., & Sweeney, L. (2015). Who know what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps.

Zetter, K. (2015, August 18th). Hackers finally post stolen Ashley Madision data. Wire