Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 88-97
Doi: 10.17645/mac.v3i2.266

Article

Literacies for Surveillance: Social Network Sites and Background Investigations

Sarah Jackson Young

Department of English, Arizona State University, Tempe, AZ 85287, USA; E-Mail: smjacks4@asu.edu

Submitted: 8 April 2015 | In Revised Form: 22 June 2015 | Accepted: 23 July 2015 |
Published: 30 September 2015

Abstract
In September 2013, civilian contractor Aaron Alexis entered the Washington Navy Yard and murdered twelve people before being fatally shot by police. This incident, together with an incident three months earlier involving Edward Snowden, caused the U.S. government to critically examine their background investigation (BI) process; because both Snowden and Alexis had supposedly slipped through the cracks of their investigations, there must be some flaw in the BI procedure. The U.S. Committee on Oversight and Reform concluded that rules forbidding "background checkers from looking at the Internet or social media when performing checks" was one of the main factors contributing to defective BIs (Report, 2014). Since the report's release, the Director of National Intelligence has been debating and trialing whether information from the Internet should be used to form a data double for BIs (Kopp, 2014; Rockwell, 2014). Using this conversation as a discussion catalyst, I argue that due to the nature of the data double, if the United States were to adopt the use of social networking sites (SNSs) for security clearance purposes, neglecting to take into account basic principles of SNSs into the process of BIs may lead to misinformation and unfavorable adjudication. Ultimately, being literate about the social practices involved in SNSs and surveillance would benefit not only investigators, but anyone, including academics, looking at individuals in online spaces.

Keywords
background investigations; data double; literacies; sorting; surveillance

Issue
This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction

In 2013 after government contractors Edward Snowden and Aaron Alexis used their security clearances for purposes other than the government intended (Snowden leaked classified information and Alexis gained access to a secured facility where he then murdered twelve people), the U.S. government began to question the BI process that allowed both to be in cleared positions with access to protected information and protected places. According to a letter in November 2013 from U.S. Representative Darrell Issa, Chairman of the Committee on Oversight and Government Reform, Issa demanded, due to the problems caused by Alexis and Snowden, that the agency which conducted both of the BIs, the U.S. Office of Personnel Management (OPM) should release "detailed information about the policies and process" that Alexis and Snowden went through for their clearances (Issa, 2013, p. 1). Issa believed that by examining these processes, problems with BI would emerge.

While Snowden became a catalyst for the procedure review, Alexis' case became the model of what was wrong with the entire process. After months of investigation on these practices, in February 2014, the Committee came out with a report detailing three major flaws to the BI procedure. The first was lack of cooperation from police departments. The second was lack of continuous monitoring. Third, "[r]egulations prohibit background checkers from looking at the In-

ternet or social media when performing checks" (Report, 2014). Each "flaw" reportedly contributed to, at least in Alexis' case, "slipping through the cracks." Even though this report was a case study of Alexis, is has become a guideline for what needs to be changed in the industry.

While each of these points merits additional conversation, the third point is the focus of this paper. The full House report called "Slipping Through the Cracks: How the D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process" details that OPM's Handbook has not changed since July 2007, and since that time, Google searches and social media sites such as Twitter and Facebook have become very popular. According to the committee, "These three social media and search sites, among others, contain a treasure trove of information about their users" (H. Rep., 2014, p. 36). The report goes on to say how unfortunate it is that the handbook denies investigators the ability to use the Internet for anything other than minimal information such as looking up business addresses. The document concludes that "[t]his restrictive policy keeps nearly every piece of information on a Subject's social networking site outside the reach of security clearance investigators" (p. 36), and the report recommends updated policies which "would allow federal investigators to pull information about Subjects from of [sic] these and other websites" (p. 37). Merton Miller, the Associate Director of OPM, addressed these criticisms and confirmed the agency was already working to include use of the Internet in investigations, and that appropriate legislation would iron out access to the sites and verification of the information from the sites. The rationalization is that the sites would assist in forming "a more complete picture of the Subjects under consideration for a security clearance than currently exists today" (p. 38). This complete picture, or data double, would then be sorted for the purpose of granting or denying the clearance.

Incorporating social media into a BI may seem like a logical step in keeping up with a candidate considering the private sector often utilizes some type of social media review (i.e., "Social Intelligence Corp," n.d.). Not everyone agrees with this move though, and the government's use of this information is being debated between agencies. While some government officials such as those in the U.S. House's Committee on Oversight and Government Reform think information from SNSs is a treasure trove of information, others, such as Miller are more cautious about the validity of that information. This tension highlights an interesting area of study for those interested in issues of surveillance. Largely overlooked in surveillance studies, the area of BIs provide a vital illustration for understanding the intersection of surveillance, social media, and policies that could pave the way for additional uses of personal information. By examining the nature of data doubles and SNSs, this paper concludes that social media literacy is needed when incorporating SNS data into a data double for the purpose of a security clearance. Otherwise, information presented in a data double may be misinterpreted to the detriment of the subject under investigation.

2. Data Doubles and the BI

For the BI, the sorting of applicants into either a clearance grant or denial comes down to a data double. According to Haggerty and Ericson (2000), data doubles are essentially deconstructed bodies which are fragmented into components and reassembled to form a kind of virtual self to be used for surveillance. Haggerty and Ericson comment that the observed body is "[f]irst it is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows. The result is a decorporealized body, a 'data double' of pure virtuality" (p. 611). The body thus gets taken apart and analyzed in different places by different methods; it is removed from its original setting, and it is then brought together again and a newly-formed way. It is no longer the body of the individual, but it contains information from that original body. The rhetoric of the data double is described in power, among many things, as shifting (Lyon, 2007, p. 114), moving freely into new representations (Gilliom & Monahan, 2013, p. 22), circulating and unknown (Haggerty & Ericson, 2000, p. 613), transcendent, and "comprised of pure information" (p. 614). The data double becomes another version of the self which is fluidly reassembled in different ways by different people in different places for different purposes.

By creating this investigative file, the U.S. government is basically creating their version of a data double for surveillance purposes. Currently, in order to obtain a security clearance or be deemed suitable for a specially designated position of public trust or national security, an individual must first go through the BI process. Applicants either fill out the December 2010 SF-86 form which is used to conduct BIs for national security positions (U.S. Office of Personnel Management [USOPM] "Questionnaire for National Security Positions," n.d.), or applicants fill out the September 1995 SF-85P form which is used for public trust positions (U.S. General Services Administration, n.d.). As of 2015, ninety percent of the US government's background investigations are conducted by OPM, and these investigations span over one hundred federal agencies (USOPM, "Background Investigations," n.d.).

The content of the SF-86 form asks for basic identifiers such as name, date of birth, place of birth, social security number, telephone numbers and email address (USOPM, "Questionnaire for National Security Positions," n.d.). Candidates also must fill out additional basic background information for the past ten years

such as their residences, education and employment histories. The form also asks for foreign travel and foreign associates, criminal history, credit information, mental health history, any history of alcohol or drug abuse, and associations with questionable organizations. The SF-85P asks similar, but fewer questions and often reduces the time accounted for to seven years (USOPM "Questionnaire for Public Trust Positions," n.d.). According to the SF-86 and SF-85P forms, the information gathered from these forms serve a basis for the subsequent background investigation, and the results of this investigation are used for adjudication purposes. The information obtained from the investigation process is then compiled in this investigative file, and the assembled content is intended to provide "the full universe of information the adjudicators can consider" (H. Rep., 2014, p. 8). This report is forwarded to an adjudicator who reviews only this investigative file. These investigations are adjudicated based, among many things, on criteria such as the applicant's reliability, trustworthiness, allegiance to the U.S., foreign influence and preference, sexual behavior, conduct, financial considerations, alcohol and drug use, psychological conditions, and use of information technology systems ("Adjudicative Guidelines," 2006). Other points of consideration are criminal conduct, security violations, outside activities, and misuse of information technology systems (H. Rep., 1999).

In terms of the investigative file for the BI, the U.S. government makes their version of the data double when they compile an investigative file on an applicant. The data double would be an assemblage of all the information gathered on the individual for the purpose of the investigation. As mentioned in the directions of the SF-85P or SF-86, this data double could be comprised of any of the required information for the form such as name, date or place of birth, residence or employment history, personal interview, and any subsequent information obtained to verify this information.

If SNS were included, details that a user would provide on a SNS align nicely with the SF-86 and SF-85P forms, especially regarding name, date or birth, city of residence, and educational background. Many of these elements are asked for and/or volunteered by SNS users. All of these elements could be compared, corroborated, or found to be discrepant from information provided by a subject during an investigation. Other things that might be identified on a SNS are things like underage drinking (H. Rep., 2014) or friendship with foreign nationals (Kopp, 2014). The SNS could be, as the U.S. House of Representatives stated, "a treasure trove of information about their users" (H. Rep., 2014, p. 36). All this information could flow into one investigative file as part of a data double.

The nature of the adjudication process though, complicates the use of a data double in a BI. To explain, as shown, the adjudicator would not be talking to the subject of the investigation him/herself; the adjudicator would just be looking at this investigative file or data double. This would be an abstracted, decorporealized body there to be sorted. Depending on what the data double was made up of, the adjudicator would decide on position suitability, and this person would be sorted into a clearance granted or denied position. This is problematic though because as Lyon (2007) reports, many times an individual may feel that their data double "does not accurately represent them" (p. 90). An individual may feel that what shows up in investigative file may not fully represent, or misrepresents, their life.

A quick example of the potential problems that the data double could lead to in the BI is alluded to in a summary report of the flaws involved in Aaron Alexis' investigation. In a press release, the U.S. Committee on Oversight and Government Reform pointed out that over 450 law enforcement departments did not fully cooperate with the OPM BI process (Report, 2014). In Alexis' case, the Seattle Police Department did not fully divulge information about a gun-related arrest, and there was also limited information provided about an anger-fueled black-out. While Alexis may have been able to get his clearance based on this lack of information, it may not go this way for others. For instance, if a clearance candidate was arrested by a law enforcement agency that did not cooperate with the investigative process, then incomplete information may only be available to an adjudicator, and the adjudicator may not be able to see that the arrest information was only a minor charge or that charges were dismissed. This incomplete information may in fact hurt an applicant. While an individual may be able to defend and respond to questions from an adjudicator about the charge, a decorporalized data double cannot answer back.

The danger of misinformation is especially true for SNSs, and adding SNSs to the BI process could offer further complications. While the above police report may have some semblance of facts, due to the nature of SNSs, information gleaned from these sites may be even less-reliable than an incomplete police report. People don't necessarily create SNSs with the intended purpose of having the government surveil them or look at the data they have posted. Users often expect to be watched, but it is most often the thought of social surveillance, or the use of social media to see what friends, family, and acquaintances are up to (Marwick, 2012), which guides their paradigm of observation. As a result of this, users don't always just report the truth or facts, and sometimes information is posted just to be entertaining. Due to the tone of the site, some users can be encouraged or feel comfortable posting information that isn't necessarily true in order to match the tone of other site interactions. For instance, according to boyd and Ellison (2008), "The extent to which portraits are authentic or playful varies across both sites; both social and technological forces shape these prac-

tices" (p. 220). Donath and boyd (2004) provide the example of a law professor on Orkut who stated his career skills were "small appliance repair" and his career interests were "large appliance repair" (p.75). In this case, this playful post didn't seem to be problematic or purposefully deceptive, but an outsider without really knowing the Subject may misinterpret the information as a falsehood if it didn't match up with other information. Misinterpretations like this may end up as a permanent record though, in one's investigative file, on the way to adjudication, and because data doubles cannot talk back, the usefulness and consequences of using this information may be detrimental to the subject of investigation. If one didn't list "appliance repair" in an employment section, they may appear dishonest. This example then brings up the importance of having some type of basic understanding, or literacy, of the practices involved in SNSs. While knowing these practices cannot verify information, they can provide an interpretive foundation for those that incorporate SNSs in to BIs.

3. SNS Literacy

According to Brian Street (1984), literacy is "shorthand for the social practices and conceptions of reading and writing" (p. 1). Knobel and Lankshear (2008) also add that literacies are "socially recognized ways of generating, communicating and negotiating meaning content" (p. 255). Implicit in these definitions is that literacy is not just reading and writing, and literacy is not just mastering a skill set or competencies. Being literate assumes that one knows the social practices that one engages in while reading and writing. Not taking into account the practices assumes literacy is neutral and not affected by situation; once someone learns to read and write, this skill will translate across every platform and situation. This is not the case though, as even a reader switching between a fiction and non-fiction text would have to understand the assumptions or practices each genre carries. Readers come to realize that fiction books are often meant to entertain rather than inform. A more robust and thorough understanding of literacy then calls for an expanded model which draws on not just skills but on the social practices and assumptions surrounding skills and spaces—all of which vary with context.

Taking information from SNSs at face value and incorporating this information in BIs/data doubles without any type of discretion or filtering process would be an example of failing to understand literacies for SNSs in BIs. Because SNSs are involved in social practices, one must be literate in the ways different assumptions alter and shape the content of SNSs. As previously discussed, an outsider looking at a SNS for the purposes other than social surveillance would already be reading SNSs out of context, and not understanding the sites' practices would further complicate any claims of objectivity. The following literacies could be used as guides for those analyzing SNSs for the purpose of BIs or any other type of analysis of SNSs. Understanding each of these literacies would be essential for the federal government or outside researchers when considering including SNS information into permanent records.

The example of Chelsea (then Bradley) Manning's Facebook page will be helpful to understand the application of these principles to SNS and BIs. Chelsea Manning was convicted in July 2013 of giving classified documents to Wikileaks. PBS's *Frontline* published an annotated version of Manning's Facebook page from the opening of his account in July 2007 to its conclusion in June 2010 ("Bradley Manning's Facebook Page," 2011). Other than Manning and Manning's ex-boyfriend Tyler Watkins, the site blurs out those that comment and post on the page. All posts listed are also those authored only by Manning with the exception of the final post on June 5, 2010 which is a post from Manning's aunt, posted under Manning's name, to let his Facebook friends know that he has been arrested. Although these posts have been annotated, what is left provides more than enough information for a case study analysis. Manning will be referred to as "he" throughout this analysis because Manning was Bradley at the time of the postings.

4. SNS Literacy and Manning

The first literacy that would be crucial to have would be functional literacy. Functional literacy of SNSs would provide a basic foundation of what a SNS even is. Selber (2004) describes functional literacy as imagining technology as a tool and participants as users. Functional literacy has often been described as mastering techniques, neutral and decontextualized out of the social sphere it exists in. A user that can maneuver around and be competent with a computer begins to be functionally computer literate. This idea is often seen in late 1990's national programs to get students ready for business in the 21st century. For instance, Cynthia L. Selfe (1999) shows that Clinton and Gore's 1996 Technology Literacy Challenge was essentially about teaching students skills on how to use a computer. A student would be literate in technology once they became competent and learned a set of finite skills. Lankshear and Knobel (2008) use the related term "standardized operational definition" (p. 3) and add this concept centers around the idea that one is digitally literate by acquiring proficiencies which may include tasks, performances, and demonstrations of skills. It involves skills like using a computer, understanding its components, and navigating the Internet. For SNSs, functional literacy could involve understanding how sites are set up and the platform limitations of them such as Twitter's 140 character limitations (while other

sites such as Facebook are without these constraints).

boyd and Ellison (2008) also identified three other functional characteristics of SNSs which aren't specific to one platform and tend to permeate the overall purpose of SNSs. The first fundamental element is that SNSs are online forums which individuals can create online presences (private or semi-private) within the constraints of a defined system. Second, SNSs organize and present a list of other users on the site which the user either knows or may have a connection with. Third, more than just aggregating a group of connections, SNSs also let users look at the profiles of these connected individuals. For a SNS review, each of these characteristics would help frame the overall analysis. The sites are not necessarily geared towards a strict recounting of life events; they are often forums to discuss thoughts with connections (public or private) or to view other associations.

An investigator who was functionally literate of a SNS would need to understand the basic functions of social media or the basic components of what makes up a SNS. While this may be the most basic of literacies, being able to understand the overall site fundamentals would be an important skill for several reasons. First, functional literacy would help an investigator understand the privacy controls of the site. Investigators, depending on what restrictions are placed on access to a SNS, would want to know if they are able to actually view a page or if they would need additional access due to technological restrictions on the access to the site. They would have also need to understand if they would have access to private messages or if they are obligated to only see public information. Functional literacy of the friends on SNSs would entail understanding the ways that someone else is allowed to provide content by posting on another's page. If one is friends with another, the friends may be allowed to submit messages on someone else's page, and this may vary across platforms. For instance, photos shared and tagged through Twitter or Instagram can be shared differently or than those shared through Facebook. It would also mean being concerned with access to the individual's friend lists. If an investigator has access to one's SNS, does that mean they are able or should be encouraged to look through the list of friends? What would be the limits of looking at related pages? And, are those friends scrutinized too? Functional literacy would help set boundaries on obtaining information.

In Manning's case, Manning set up this Facebook page according to Facebook's constraints. Investigators would have wanted to understand that when Manning set up his page, only certain elements can go on that page in certain ways. For instance, Manning's first post on July 22, 2007 states, "Just created a new Facebook" ("Bradley Manning's Facebook Page," 2011). Through the timeline, Manning posts numerous other general comments such as July 27, 2008's post stating, "Home today" or August 6, 2007's "back home from Lollapalooza." Each post is identified as being Manning's by having his photo and name next to it. Throughout the timeline he also posts photos of himself like December 24, 2007's photo captioned "Just Me" and URLs such as June 28, 2008's link to Bob Barr's 2008 campaign. Facebook places the individual's name and photo next to each post, and it allows content like text, photos and hyperlinks.

Also, it would need to be understood that these are Manning's public posts (or at least public to his friends), and while these messages may have been observable to some or all of Manning's connections, they may not be observable to everyone. Facebook allows users to limit the audience of posts from the broad public to specific users ("When I post something," 2015). Additionally, there is also the messenger function which allows direct messages between users or groups of users. Investigators would need to know their information limitations.

It is important too, to understand that Manning's contacts are also able to contribute to Manning's page. For instance, on February 24, 2009, a redacted individual posted "Hahahah ah I c" and May 26, 2009 another redacted individual posted, "Ditto" ("Bradley Manning's Facebook Page," 2011). While these posts are not seemingly consequential, they do highlight others can post on the site, and posts like this bring up the question of association. If someone wrote something inappropriate, would Manning have been responsible for those quotes even if he didn't agree with them if they weren't deleted? It is also worth noting that Manning's last entry, according to *Frontline*, was posted by his aunt and read, "Some of you may have heard that I have been arrested for disclosure of classified information to unauthorized persons…" This also begs the question of the authenticity of any of the posts; while it may be Manning's page, Manning may not have been the direct poster of the entry if someone else had access to the account.

Overall then, Manning's site shows that due to the system architecture, for an outsider to understand the content of SNSs, one such as investigator would want to know functional matters like what specific technological constraints could influence the information that is contained on the site. This would matter regarding presentation of the site, privacy of the site, and contributions to the site. While this literacy may seem the most basic of understandings, it would be important to understand these elements even begin to start to decipher the information taken from a SNS.

A second literacy is rhetorical literacy. Bizzell and Herzberg (1990) relay that one understanding of rhetoric is "the use of language, written or spoken, to inform or persuade" (p. 1). Language is thus used to produce spaces in which the orator or writer creates areas of in-

fluence. According to Rheingold (2012), those posting in SNSs such as Facebook or Google+ are such participants which "seek, adopt, appropriate, and invent ways to participate in cultural production" (2012, p. 19). This participation can be anything from making a post to remixing or recreating a popular video. For Erstad (2008), being able to participate represents a shift in society from spaces that are defined by others to places where the audience can take "available content and create something new, something not predefined" (p. 178). SNSs are places where this rhetorical production happens. Users, through the constraints of a defined system, are able to create a space of their own. Having a rhetorical literacy would then entail examining the design and evaluation of these online spaces with the idea in mind that users are producers of their environments.

Further, these users don't just produce for themselves, and rhetorical production takes place in front of spectators. On SNSs, users write in certain ways for certain perceived audiences. For SNSs, a list of friends on the site can be understood as an audience. The SNS audience serves a meaningful function because this "public display of connections" (Donath & boyd, 2004, p. 72) is essential in helping shape the content of posts. Having connections on these sites presents a public for the user (Baym & boyd, 2012). The users are no longer just interacting with an unknown audience; they are interacting with a specific public where for the most part they are aware of the groups' identities. This imagined audience further causes a user to engage in behavioral norms (boyd & Ellison, 2008), and based off the users' perceived associations, the user may adapt the message they are delivering. This awareness of a public in social media also changes how people write (Baym & boyd, 2012). When dealing with connections, a person may vary what they say due to their imagined audience of their connections (boyd & Ellison, 2008). According to Donath and boyd (2004), "Knowing that everyone they interact with knows of and can communicate with a group of their acquaintances can influence their behavior" (p. 76). Further, people adjust what they are going to say based off of their audience (Baym & boyd, 2012). When SNS users are creating their profiles and constructing their identities, "they must consider how they will be received by their intimate publics and also how the public telling of their stories might affect their loved ones" (p. 324). Because of these tailored messages, an outsider would thus want to understand the values that the site and friends have and their influence upon the user's posts. Rhetorical literacy then would entail also understanding the intended audience of a SNS.

For Manning and rhetorical literacy, Manning was a producer of a site in front of his audience. It was often clear that he was writing for groups of friends and family. His aunt would have been aware of his site because she posted his final message, so his aunt was among his audience. Additionally, he addressed certain groups of people on certain occasions. On December 17, 2009, Manning states, "Thanks for all the birthday wishes at my double deuces" ("Bradley Manning's Facebook Page," 2011), and two days later he wrote, "[T]hanks everyone for all the goodies. I've been getting them! Hope to write everyone." Earlier in the year on July 4, 2009, Manning put the word out that "[Bradley Manning] needs 4th of July plan for D.C. Call me." On December 24, 2008, he "wishes you all a Merry Christmas," and on July 27, 2007, he remixed a Fergie song and asked, "[I]'d like y'all to give me some feedback." On other occasions, he singled out Starbucks coworkers such as the July 26, 2007 post addressed, "STARBUCKS PEEPS." Each of these points presents good examples of Manning addressing specific audiences. Manning did not appear to be posting random thoughts for outsiders to peruse; instead, these posts seem to be directed towards an audience that he knew personally.

While is impossible to know how Manning's posts were adapted to his audience without a direct conversation with Manning, research does show that the content of posts are influenced by site practices and the audience. Understanding Manning's audience may be a key to understanding where important information is for investigators. According to Baym (2010), "Any instance of digital language use depends on the technology, the purpose of the interaction, the norms of the group, the communication style of the speaker's social groups offline, and the idiosyncrasies of individuals" (p. 65). Thus, people write in certain ways through specific technologies for certain audiences. The postings then are not acontextual occurrences. People are aware that others are looking at them and may "feel pressured to conform to those groups' norms" (p. 81). It is thus interesting then to consider why Manning gave information to Wikileaks and also, according to *Frontline*, was reprimanded by the Army "for revealing sensitive information in video messages to his friends and family posted on YouTube" ("Bradley Manning's Facebook Page," 2011), but he did not do the same on Facebook. Audience awareness then would help signal where possibly more telling information would be divulged. For some reason, Manning was more motivated to share sensitive information with his audience on platforms other than Facebook.

A third literacy would be informational literacy. This literacy would be a key skill involved in SNS use for the BI. Informational literacy deals with being able to locate, be critical of, and use information found by digital means. Being discerning about information would determine what information was important and should be included in one's data double. For Fieldhouse and Nicholas (2008), information literacy draws on using critical thinking skills in order to decipher information

from multiple, competing sources. Since SNSs often provide an overabundance of information, being able to decipher that information would be exceptionally important. Howard Rheingold's (2012) idea of crap detection fits well into this understanding of literacy. Rheingold outlines that a necessary digital literacy is to navigate through the crap that may be present on the web in order to find and use the most accurate and relevant information. This involves looking at authors, identifying publishers, and making sure information is corroborated by other sources. Rainie and Wellman (2012) touch on the same idea with their idea of skepticism literacy. They encourage that one should be able to assess the information from multiple sources in order to "weed out the media and people who have outdated, biased, incomplete, and agenda-driven or just dead-wrong ideas to pass along" (p. 274). Being cynical about the information presented then is essential then to SNS surveillance. This literacy asks the viewer (or in this case investigator) to use discretion in the information obtained on a SNSs.

For investigators involved with surveilling social media, understanding what information is valid is important. OPM's Merton Miller begins to explore the question of validity in the February Alexis report. Even though OPM was cooperating with the US House about considering whether to incorporate SNSs into the BIs, Miller himself pushed back on the incorporation of this information. Although Miller acknowledged that there may be value in looking at social media sites to identify things such as underage drinking, Miller resisted the committee's unrestrained approval of incorporating the information by making the following statement:

> Now, so what is the veracity of that information? You wrote it. You posted it. Somebody is going to have to determine the reliability of that. So that's the hard part, I think, in applying the social media role in background investigations. *It's not collecting it, it's not finding it, it's then doing the analysis, because when you run an investigation you shouldn't be incorporating information that isn't true about the subject in that investigation.* (H. Rep., 2014, pp. 37-38, emphasis in original)

This conversation and Miller's concerns raise a topic of conversation for surveillance studies to explore. While much analysis of Miller's statement can be conducted, on the surface, his comments at least start to pull back the House's larger prevailing notion that social media is a treasure trove of information about a subject.

For Manning's Facebook page, there were several things that could have been of interest for his BI. One category was the more benign but informational data. First there is the list of Manning's connections. According to the House report, this information could be used for lead purposes (H. Rep., 2014). Additionally, Manning provided basic working and living information. For instance for employments, on July 24, 2007, Manning states, "[Bradley Manning is] working at Starbucks," and on July 27, 2008 he announces, "[Bradley Manning is] working at Abercrombie & Fitch." ("Bradley Manning's Facebook Page," 2011). For residences, on December 31, 2007 Manning posts, "[Bradley Manning] is going back to Ft. Leonard Wood on Thursday," and on April 4, 2008 he states, "[I]'ve now moved on to Fort Huachuca in AZ." He also lists deployment locations such as October 29, 2009's post, "[Bradley Manning] has arrived at destination in Iraq." Since the security forms ask for employments and residences, Manning's mentioning of both could be used to corroborate information he listed on his paperwork.

Second, there was also other, possibly more derogatory information that could be found. For instance, Manning alludes to problems at employments. On November 5, 2007, Manning posts, "[Bradley Manning] is still in the Army, but suspended with injuries from Basic Training." Although it was for medical reasons, Manning still relays that he was suspended from the Army. He alludes to other employment problems, residence problems, and the feeling of living a double life in a November 17, 2008 entry. On this day, Manning posts a link to a news story and states, "I got an anonymous mention in this article. How fun!" The article links to an article on *Syracuse.com* in which an anonymous soldier (identified as Manning by *Frontline*) reveals, "I was kicked out of my home and I once lost my job," and also, due to the Army's don't ask, don't tell policy, ""I've been living a double life….I can't make a statement. I can't be caught in an act" (Her, 2008). Along these lines, many of Manning's posts openly speak of homosexual relationships which were not allowed at the Army at the time. For instance, in December 2008, Manning updated his Facebook page to announce, "Bradley is in an open relationship with Tyler Watkins." ("Bradley Manning's Facebook Page," 2011). While not problematic now, at the time it was against military policy. It bothered Manning enough that he admitted under the condition of anonymity that it caused him to feel like he was living a double life. Manning also spoke of his desired use of alcohol, and on his twenty-first birthday on December 17, 2008, he states, "[Bradley Manning] wants to get out of upstate, hit the clubs and get wasted as soon as possible!" Other statements which could be interpreted as questions of mental health were Manning's more dispirited-sounding posts. For instance, on May 5, 2010, he posted, "[Bradley Manning] is beyond frustrated with people and society at large." On April 30, 2010 he posted, "[Bradley Manning] is now left with the sinking feeling that he doesn't have anything left…" On March 10, 2009, he states, "[Bradley Manning] feels ignored by society." Each of these posts may lead some to believe Manning was feeling less than happy with life.

In order to determine the relevancy of any of these postings, some sort of established standards on information would be needed. While many of these discussed points may have been of interest to corroborate off Manning's security application or bring up questions of character, it is questionable if these would have flagged him as being a national security threat. If these elements were not on his form, he could have been flagged as being dishonest, but dishonesty regarding few things does not necessarily equate to divulging classified information. In light of functional and rhetorical literacies, too, the content of these posts are often influenced by external factors like the constraints of the site or the audience one is addressing. Just because Manning felt "frustrated with people and society at large," that doesn't meant that Manning would going to commit a heinous act; oftentimes people uses SNSs to interact with peers and receive feedback (Pempek, Yermolayeva, & Calvert, 2009) or for emotional support in times of stress (Baym, 2010). Information literacy then would be important when understanding what information is true, important and accurate and what information may be less consequential to a BI.

5. Discussion

The points at which humans make assumptions or submit "data" is an important place to analyze. In *Science in Action*, Latour (1987) encourages attention not necessarily be paid to the final product of scientific research, but instead, attention should be made in the negotiation of the process of production. Latour refers to the finished product as a black-box, a place where practices and assumptions are taken as given. Important to him instead is to look at the places where meaning-making is inscribed before the black-box is closed. Similarly, for those studying surveillance of SNSs, the practices involved in meaning- making then would be important points to examine.

As shown, when dealing with SNSs for surveillance, meaning occurs before an investigator even draws conclusions. Those posting in SNSs are engaged in practices that influence the production and outcome of their "completed," black-box profiles/investigative files/data doubles. These influences imbedded in these final products would in turn be more solidified as in investigator uses that black-box profile for their own analyses-turn-black-box investigative file. The adjudicator would further add their interpretation on the report for the determination of a clearance. Each point of scrutiny further inscribes more meaning.

This is especially true for any outsider (i.e., one who knows little background information about the Subject). Without knowing the exact meaning of posts, an outsider doing a content analysis of a SNS may not understand the practices an SNS user is engaged in. Research shows that most users are on SNSs to maintain already existing contacts (boyd & Ellison, 2008). A peer then would, for the most part, be someone that had a least a little context of who was being examined. An investigator or any other outsider, however, would be someone with little or no prior knowledge of the Subject or associations. This lack of context positions the outsider as an agent of surveillance compiling information about a Subject based on minimal, if any, perspective on the Subject other than the SNS profiles themselves. For investigations, this outsider status may even be favored; for instance, the idea of an impartial outside observer without close personal ties to a subject of investigation is usually the preferred construct. Just the term conflict of interest in law enforcement would imply an unwanted situation. In reality though, this lack of context may actually make it harder to identify the veracity of the information presented.

This lack of perspective for SNS may make achieving SNS objectivity in a BI difficult, problematic, and possibly with lasting consequences. In the context of BI's, surveillance information from SNSs could be solidified into the data double and used for sorting. This could all be based off of information that is influenced by social practice and needs to be verified and validated. The ramifications of not getting a clearance are strong, and a denial just one time may jeopardize an individual from future employment; question 25.2 on the SF-86 form asks if one has been denied a clearance (USOPM, "Questionnaire for National Security Positions," n.d.). Ultimately, then, any assumptions about SNS information based on a content analysis may be less than accurate. However, as Bowker and Star (1999) remind us, though, validity does not always matter. They state, "Equally, as good pragmatists, we know that things perceived as real are real in their consequences" (p. 53). The data double, full of investigative information, could come to be more real than the actual individual under consideration for a clearance. This is why a basic understanding of SNS literacies would be essential to even begin to use SNSs in BIs.

6. Conclusion

Civilian and government agencies use and contemplate using social media assemblages as part of their version of a data double. Looking at the nature of social media through a literacies lens shows though that many times the individual in control of a SNS profile manipulates that profile due to the constraints and norms of the communities they are part of. While this does not necessarily mean social media profiles are deceptive, it does make one question the incorporation of SNSs into the BI process which would have real consequences for those denied a position due to information on a SNS. Due to the importance of these ramifications, it would be beneficial then for those doing surveillance to have

a solid understanding, or literacy, of the functional matters of what social media is comprised of, the practices it engages in, what is created and for whom, and how users and investigators shape interpretations of social media profiles. Beyond the BI, this would be important for any outsider trying to surveil SNSs for any purpose. Even academics using SNSs as spaces of study would want to be literate of these sites.

While this paper raised the need for literacies, it did not go into more specific criteria could be used. Further research into appropriate and relevant criteria would need to be conducted. The conclusions of this paper lead to a desire for more analysis of ethical considerations and of what policies should be used for examining a SNS for the purpose of the BI data double. Not understanding social network limitations ultimately may affect the sorting of profiles and eventual acceptance of employment, and as SNSs grow in popularity, these questions only become more important.

Acknowledgments

I wish to thank the anonymous reviewers for this journal and the Rhetoric, Secrecy, and Surveillance participants at the Rhetoric Society of America's summer institute for feedback on earlier versions of this paper.

Conflict of Interests

The author declares no conflict of interests.

References

Adjudicative guidelines for determining eligibility for access to classified information. (2006, February 3). Retrieved from http://www.state.gov/m/ds/clearances/60321.htm

Baym, N. (2010). *Personal connections in the digital age*. Cambridge: Polity Press.

Baym, N., & boyd, d. (2012). Socially mediated publicness: An introduction. *Journal of Broadcasting & Electronic Media, 56*(3), 320-329.

Bizzell, P., & Herzberg, B. (1990). *General introduction.* In P. Bizzell & B. Herzberg (Eds.), *The rhetorical tradition: Readings from classical times to the present* (pp. 1-15). Boston: Bedford Books of St. Martin's Press.

Bowker, G., & Star, S. (1999). *Sorting things out classification and its consequences*. Cambridge: MIT Press.

boyd, d., & Ellison, N. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*, 210-230.

Bradley Manning's Facebook page. (2011, May 24). Retrieved from http://www.pbs.org/wgbh/pages/frontline/wikileaks/manning-facebook-page

Donath, J., & boyd, d. (2004). Public displays of connection. *BT Technology Journal, 22*(4), 71-82.

Erstad, O. (2008). Trajectories of remixing: Digital literacies, media production, and schooling. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 177-202). New York: Peter Lang.

Fieldhouse, M., & Nicholas, D. (2008). Digital literacy as information savvy: The road to information literacy. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 47-72). New York: Peter Lang.

Gilliom, J., & Monahan, T. (2013). *SuperVision: An introduction to the surveillance society*. Chicago: University of Chicago.

H. Rep. (1999). *Report to the Ranking Minority Member, Committee of Armed Services. Inadequate personnel security investigations pose national security risks*. No. 05-552. Retrieved from: http://www.gao.gov/products/GAO/NSIAD-00-12

H. Rep. (2014). *Committee on Oversight and Government Reform. Slipping through the cracks: How the D.C. Navy Yard shooting exposes flaws in the federal security clearance process*. Retrieved from http://oversight.house.gov/wp-content/uploads/2014/02/Aaron-Alexis-Report-FINAL.pdf

Haggerty, K. D., & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622.

Her, P. (2008, November 17). Teen hears peoples' stories at LGBTQ rally. Retrieved from http://blog.syracuse.com/voices/2008/11/teen_hears_stories_at_lgbtq_ra.html

Issa, D. (2013, November 20). Letter to US Office of Personnel Management. Retrieved from http://oversight.house.gov/wp-content/uploads/2013/11/2013-11-20-DEI-to-Archuleta-re-in-camera-review-due-11-21-13.pdf

Knobel, M., & Lankshear, C. (2008). Digital literacy and participation in online social networking spaces. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 249-278). New York: Peter Lang.

Kopp, E. (2014, October 10). Social media could become part of security clearance process. Retrieved from http://www.federalnewsradio.com/502/3730507/Social-media-could-become-part-of-security-clearance-process

Lankshear, C., & Knobel, M. (2008). Introduction. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 1-16). New York: Peter Lang.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Cambridge: Harvard University Press.

Lyon, D. (2007). *Surveillance studies: An overview.* Malden: Polity Press.

Marwick, A. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society, 9*(4), 378-393.

Pempek, T., Yermolayeva, Y., & Calvert, S. (2009). College students' social networking experiences on facebook. *Journal of Applied Developmental Psychology*, *30*, 227-238. doi:10.1016/j.appdev.2008.12.010

Rainie, L., & Wellman, B. (2012). *Networked: The new social operating system*. Cambridge: MIT Press.

Report: D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process. (2014, February 11). Retrieved from http://oversight.house.gov/release/report-d-c-navy-yard-shooting-exposes-flaws-federal-security-clearance-process

Rheingold, H. (2012). *Net smart: How to thrive online.* Cambridge: MIT Press.

Rockwell, M. (2014, November 6). Should social media affect your security clearance? Retrieved from http://fcw.com/articles/2014/11/06/odni-social-media-monitoring.aspx

Selber, S. (2004). *Multiliteracies for a digital age*. Carbondale: Southern Illinois University Press.

Selfe, C. (1999). *Technology and literacy in the twenty-first century: The importance of paying* attention. Carbondale: Southern Illinois University Press.

Social Intelligence Corp. (n.d.). Retrieved from http://www.socialintel.com

Street, B. V. (1984). *Literacy in theory and practice*. Cambridge: Cambridge UP.

U.S. General Services Administration. (n.d.). GSA Forms Library. Retrieved from http://www.gsa.gov/portal/forms/download/116382

U.S. Office of Personnel Management. (n.d.). Background Investigations. Retrieved from http://www.opm.gov/investigations/background-investigations

U.S. Office of Personnel Management. (n.d.). Questionnaire for National Security Positions. (OMB Publication No. 3206 0005). Retrieved from http://www.opm.gov/forms/pdf_fill/SF86pdf

U.S. Office of Personnel Management. (n.d.). Questionnaire for Public Trust Positions. (OMB Publication No. 3206-0191). Retrieved from http://www.opm.gov/Forms/pdf_fill/sf85p.pdf

When I post something, how do I choose who can see it? (2015). Retrieved from https://www.facebook.com/help/120939471321735

About the Author

Sarah Jackson Young

Sarah Jackson Young is a former government contractor, Teaching Associate, and fourth year PhD student in the English—Rhetoric, Composition, and Linguistics program at Arizona State University. She previously examined the Internet presence of the U.S. Department of Homeland Security during her MA, also in Rhetoric and Composition at Arizona State. Her current research interests are surveillance studies, background investigations, and use of the Internet for surveillance.