Article

Slipping Through the Cracks: Background Investigations after Snowden

Sarah Young

Arizona State University, USA.
smjacks4@asu.edu

Abstract

Although Edward Snowden set out to expose the extent of the United States (US) government's surveillance practices so that the public would be aware of the magnitude of the country's information gathering, Snowden's actions have actually, at least in the case of background investigations, revealed an inability for the US government to gather all desired information for surveillance purposes. This lack of ability to gain access to information has several major consequences. First, it has created a call for more information to be gathered. It has also affected federal workers' privacy and whistleblowing capabilities, encouraged a false trust in a fallible system, and has perpetuated the belief that the BI can actually capture the essence or "whole person" of an individual so much that it can tell the future. All of these elements are problematic and help show how surveillance proliferates in modern society.

Introduction

Background investigations (BIs) are ways the government controls risk. In order to make sure those with access to classified data will not divulge this information, BIs employ surveillance by gathering an assemblage of information that combines to create a supposedly accurate picture of the clearance candidate, or also called the "whole person" representation of a subject of investigation. This "whole person" is judged by an adjudicator to make a determination as to whether the individual should or should not have access to classified information.

By looking at an investigation based on the "whole person" concept, Edward Snowden was supposedly cleared as non-threatening. Once Snowden divulged classified information though, the BI practices were called into question because somehow Snowden must have slipped through the cracks; otherwise, a properly cleared individual would not have committed those actions. As a result of Snowden's revelations, US Congress launched an investigation into the BI process. After months of investigation, and subsequently combined with investigations into the actions of another security incident involving Aaron Alexis two months later, Congress concluded that not enough information was being obtained on those with security clearances.

So, although Snowden set out to expose the extent of US government's surveillance practices so that the public would be aware of the magnitude of the US's information gathering, Snowden's actions actually, at

least in the case of BIs, started a conversation that revealed an inability for the US government to gather all desired information for surveillance purposes. Consequentially, this motivated Congress to call for more surveillance. This call has ramifications not just for increased monitoring, but the calls have implications for federal workers in areas such as privacy and whistleblowing, encouraged a false trust in a fallible system, and has perpetuated the belief that the BI can actually capture the essence or “whole person” of an individual so much that it can tell the future. Each point provides justification to increase surveillance.

Surveillance and Risk

When studying risks, at least three positions emerge in risk scholarship. Realists and those taking the cognitive science perspective argue that risks are real and can be identified and predicted using scientific methodology (Lupton 1999). Fields typically taking a more technico-scientific approach to risk are engineering, statistics, or economics, and those employing these positions think in terms of probabilities and consequences. On the other hand, cultural relativists (Ekberg 2007) and strong constructionists (Lupton 1999) argue that there are no risks in themselves, and risks only exist because of practices of analysis. Risks are only deemed risks through social and political positioning. This isn't to say those taking this perspective don't think there are external harms; often the term “risk” may be thought of in a different way. For instance, what some may consider risks, others may just consider hazards or dangers (Ekberg 2007; Fox 1999). Weak constructionists (Lupton 1999) and risk society theorists take more of the middle ground and hypothesize that risks exist because they are real and can do harm (Ekberg 2007; Lupton 1999), but they are also “*open to social definition and construction*” (Beck 1992: 23). This stance then recognizes that risks do exist, but they are also influenced by the cultural contexts which change through time. Risks exist but can never be separated from social and cultural processes (Lupton 1999: 35). This essay will take the position that risks exist, but they are socially, culturally, and politically influenced.

That risks are something to be avoided is a modern idea. Before our modern period, risks were considered a neutral term that implied a more general idea of the potential for loss or gain (Fox 1999: 12). While risk can still be seen as positive for those such as explorers who brave danger (Giddens 1999), in more recent times, risk is a label placed on something negative, threatening, a deviation from the norm, or an undesirable event (Ekberg 2007; Lupton 1999). Two theorists, Ulrich Beck and Anthony Giddens, provide much discussion in the area of socially and politically influenced ideas of risk. In Beck's (1992) book *Risk Society: Towards a New Modernity*, Beck argues that today's risks are the results of modernization. These new risks are different enough from the past that Beck concludes we are now living in a *risk society*. According to Giddens (1999), a risk society is a society not that is more dangerous than in earlier times, but “is a society increasingly preoccupied with the future (and also with safety), which generates the notion of risk” (1999: 3). Giddens continues that this risk society has emerged because modernized society is no longer connected to nature or tradition in that we no longer worry about what nature will do to us but rather what we can do to nature, and also, we no longer follow traditions or believe we are subject to fate. Because we live in this post-nature/tradition society, our risks are what Giddens calls *manufactured*. Manufactured risks are risks where we don't have historical precedence as to what is considered risk or what could be considered a traditional response to that risk. Because of this, the decision as to whether something is or is not a risk becomes a political matter, and certain risks are emphasized and privileged over others. People are influenced towards what risks to pay attention to. In this sense then, risks become social constructions. The risks that exist are the ones society has decided to focus its attention towards.

A discussion of risk and surveillance can be seen through the idea of the control society. Contemporary power (e.g., corporations and capital) circulates in ways that are no longer limited to one place (Deleuze 1992) which creates fragmented and dispersed networks (Nadesan 2008: 5). These networks are often controlled by technology, and as opposed to a disciplinary society conceptualized by strong institutional

forces in fixed spaces, technology can transcend institutional boundaries and leave society under constant control (Lyon 2007: 60). These technological, constant forms of control are forms of surveillance and are able to reach places in citizens' lives previously not scrutinized, and society is expected to self-monitor from this constant control. Surveillance can vary from the "soft" security cameras and behind-the-scene design of physical spaces for surveillance to the "hard" obtrusive, more confrontational practices that may assume guilt like sensor gates at the exits of businesses, random drug tests, lie detector tests, and metal detectors (Staples 2000: 2-3). These practices all work together to manipulate and deter future behavior.

Beyond these soft and hard practices though, social sorting is another way in which surveillance practices attempt to manipulate the future. Social sorting can be viewed through the idea of surveillant assemblage, and the idea of assemblage can be seen in Deleuze and Guattari's theories where seemingly disparate objects come together to function as a group (Haggerty and Ericson 2000). Assemblages are not fixed and solid groupings; they are flows of information that can be reconstructed in different ways to form different assemblages. Building off Deleuze and Guattari, Haggerty and Ericson discuss that surveillant assemblages are constructed of seemingly unrelated data flowing from multiple sources that are "reassembled and scrutinized in the hope of developing strategies of governance, commerce and control" (2000: 613). Surveillant assemblages are fundamentally different than popular surveillance metaphors like Big Brother and the Panopticon which rely on centralized and singular entities. For Big Brother, there is a totalitarian state looking at everyone's movement, and for the Panopticon, there is a single site of brick and mortar observation (Gilliom and Monahan 2013: 22). Surveillant assemblages on the other hand expand surveillance from the idea of one watcher to a larger network and flow of information coming from multiple places. Assemblages obtained through surveillance can be reassembled into data doubles (or various iterations of one's assembled digital personal data) (Lyon 2003: 22), and these data doubles can be categorized into groups which grant advantages or disadvantages due to their categorization.

These data doubles are also subject to social sorting through technological means. Lyon explains that social sorting is enabled by the "use of searchable databases and associated techniques such as data mining, characterized by the classifying and profiling of groups in order to provide different levels of treatment, conditions or service to groups that have thus been distinguished from one another" (2009: 41). This means that people are sorted into certain groups for the determination of advantages or disadvantages. Gandy's (1993) idea of the panoptic sort described as an "all-seeing eye of the difference machine" designed to sort people based on routine measurements in order to provide or deny opportunities (1993: 15) speaks to the same theoretical construct. Machines use assembled data to categorize types which results in gains or losses for an individual or group. Oftentimes, the data or risk factors used to sort people are features people have little control over such as information based on "age, race, ethnicity, gender, and chronic disabilities" (Ericson and Haggerty 1997: 120).

Law enforcement is one area that uses technological sorting to anticipate behavior, and in policing, categorization can lead to suspicion of crime. Marx (1988) theorizes that there is a new surveillance taking shape which draws power from the combination of centralized and decentralized powers where information from both private corporations and governments work together to use computerized data to safeguard communities. These "maximum security societies" involve developments such as the proliferation of the use of computer records and the growth of actuarial approaches based on the predictions of future (Lyon 2007: 38). Data generated through surveillance produce "types" that are at "risk" for behavior despite if the person has ever committed that type of behavior (Staples 2000: 6). Those found to be most at risk are under more scrutiny, and being in a risky category may discount some people from future prospects by contingently categorizing them as guilty until proven innocent (Lyon 2007: 38). Robert Castel calls this type of surveillance "systematic predetection" (1991: 288), and instead of addressing concrete situations of peril, it tries to anticipate future danger. Preventative policies attempt to assemble elements which could be risky at a later date to make these future risks identifiable and visible in the present.

Law enforcement is one institution responsible for creating its own system of risk management. In Ericson and Haggerty's (1997) *Policing the Risk Society*, the authors take a constructivist approach to this management by stating, "Risks exist only in institutional knowledge about them" (1997: 100). Institutions define what risks are, and they essentially call themselves into being with constitutive risk rhetoric. In establishing risks, institutions establish what risks mean, determine classification standards, and define how they will react to them. Risks then connect to risk communication systems which relay and make visible the risks of the institution through systems of rules and formats, and this communication further establishes appropriate narrative writing structures for reporting on risk. This institutionalism moves the authorship of risk away from the individual and to the routinized, institutional expectations. These standardizations allow the information to be compared to similar institutionalized information. Risk professionals then can interpret and rationalize these visible risks to further enforce institutional standards.

Risk, Surveillance and Background Investigations

In the context of this discussion of risk, BIs can be seen through a constructionist approach. As will be explored, BIs are the US government's way of constructing/defining what is (and what is not) a risk. They are also hard, confrontational forms of surveillance which make clear indication an individual is under surveillance: individuals subject to these investigations fill out large application packages, are aware and are given directions that many of their connections could be contacted, and sign consent forms for information to be obtained (US Office of Personnel Management [USOPM] 2015d). They are also future-oriented surveillant assemblages piecing together information from a variety of sources designed to be used to sort the subject of investigation into the good category of non-threatening which would result in access or the bad category of too-risky which would result in a clearance denial. Looking at the following information will help show these conclusions.

According to the White House, BIs are composed of two components: investigative and adjudicative measures, and "a security investigation is defined as any investigation required for eligibility to hold a sensitive national security position or access to classified information by military, civilian, or government contractor personnel performing work for, or on behalf of, the government" (Office of the White House 2014: 2). To limit access to classified information, the government organizes proprietary information into a hierarchy at three main levels: Top Secret (TS), Secret, and Confidential. Agencies require a BI in order to access this information. The damage of unauthorized disclosure of information is expected to harm national defense and foreign relations with the levels of "exceptionally grave damage" for TS information, "serious damage" for secret information, and "damage" for confidential information (Government Accountability Office [GAO] 1999: 5). Each designation is designed to compartmentalize information to allow only persons cleared at the appropriate level access to information. In this process, each candidate is essentially contingently categorized, a concept which Lyon brings out means one is "suspect until the system clears the way to entry" (Lyon 2007: 38). Once approved, the candidate obtains the clearance and can access the permitted level of information.

Formerly managed by the US Office of Personnel Management's (OPM) Federal Investigative Service division (USOPM 2015a), as of October 1, 2016, over 95 per cent of the BIs for the US government are now conducted by OPM's National Background Investigations Bureau (USOPM 2016). This bureau works with over one hundred agencies and provides organizations adjudications, trainings, and reports of investigation. Because OPM handles the majority of the investigations to include Edward Snowden's BI (Brickley 2015), the focus of this analysis will be on OPM.

The BI is made from an assemblage of different elements such as an interview with the candidate, proof of date and place of birth, corroboration of education and employment, interviews with coworkers and neighbors, national agency checks, financial review, law enforcement checks, and many other different factors (GAO 1999: 10; GAO 2000: 3). These components are then transmitted through the government's

risk communication system by placing them into a report (which moves the authorship of risk away from the individual and to the routinized, institutional expectations), and this report becomes a simulacrum or data double of who the candidate supposedly is (Young 2015). To make a determination for clearance fitness, once these parts are assembled, an adjudicator, or risk professional, looks at the subject of investigation's "whole person" by analyzing the assembled information (US House of Representatives Committee on Oversight and Government Reform [USHRCOGR] 2014b: 19). Through predetermined institutional risk factors, the adjudicator looks for things like allegiance to the United States, foreign influence, sexual behavior, personal conduct, finances, use of alcohol or drugs, mental and emotional health, criminal conduct, security violations, and misuse of information technology systems (GAO 1999: 10-11). At the end of the process, without personally meeting the subject under consideration for the clearance (USHRCOGR 2014b: 38), the adjudicator decides if the candidate gets the clearance. Overall, these clearance classifications are important to minimizing risk because, as Lyon brings out, classifications are ways which power is maintained and constructed. Classification "makes several entities known in particular ways" (Lyon 2007: 84) which makes entities easier to control. In the risk construction of BIs, adjudications make it clear who to trust and who to doubt in order to manage and control people and information. The designation is then maintained through a database such as the Joint Personnel Adjudication System, Scattered Castles (Loveridge 2012), or the Defense Information System for Security (Hakamaa 2016) to keep track of who has a clearance.

Snowden, Background Investigations, and Calls for Reform

So, if BIs are constructed as the way to minimize the risk of causing damage to the country, then Snowden broke the narrative of BIs by doing the thing that the BI was supposed to eliminate. Jon Tester of the US Senate said those giving away sensitive government information do an "untold damage to our national security" and show the failure of the BI process (US Senate, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Committee on Homeland Security and Governmental Affairs 2013: 2). Snowden was one of those people giving away information. Instead of keeping information to himself, he divulged sensitive government information to the media and in turn the public.

Snowden's purpose was to not to show the weakness of the BI system though; it was to disrupt the whole system of surveillance. As discussed by Scheuerman (2014: 612), Snowden admitted that divulging classified information after signing a non-disclosure contract would be in violation of this agreement, but he did it anyway to expose what he felt were the unconstitutional injustices of NSA. *The Guardian* reported Snowden as stating, "My sole motive is to inform the public as to that which is done in their name and that which is done against them" (Greenwald, MacAskill, and Poitras 2013). Snowden, formerly a watcher and surveillance-worker, flipped the dynamic of the watched and the watchers. In the face of fundamental principles of surveillance which sees surveillance as "observational rather than interactive" (Jenkins 2012: 162) and asymmetric (Andrejevic 2006: 396; Marwick 2012: 380), Snowden took propriety surveillance information to a public forum for the public to see. He did this not just to show what was being done but also to start a larger conversation. Snowden continues, "I really want the focus to be on these documents and the debate which I hope this will trigger among citizens around the globe about what kind of world we want to live in" (Greenwald, MacAskill, and Poitras 2013). Snowden wanted the world would see what was happening and question the amount of surveillance being obtained.

Regardless of his intentions though, in the context of BIs, Snowden did something that BIs were supposed to prevent, so therefore he signified a problem with the system. Because of this, Snowden is even said to embody the idea of "slipping through the cracks." This idiomatic expression of slipping through the cracks usually means that someone fell through a system's control. It implies that there was an airtight system in place, and someone was able to get through the normally impenetrable processes that should have prevent an individual for doing what he/she did. While the expression may take different forms, it is usually

something negative. For instance, for a child “slipping through the cracks” of a family welfare department or educational system means something bad has probably happened to the child be it e.g., an injury or not being able to read. In this case, the system has failed the child, and the child is seen more as the victim. For a criminal “slipping through the cracks” of the justice system may mean a criminal has committed a crime, but due to some systemic flaw like lack of paperwork the individual is e.g., not arrested or somehow can flee the country to avoid arrest. In the case of a criminal, the system has failed the public, and the criminal is the swindler that somehow found his way around a normally effective system. Snowden’s case takes more of this second example. For Snowden, slipping through the cracks implies that there were measures in place, but somehow the system failed which put the public at harm. In the context of BIs, Snowden is seen as the villain who fell through the safeties in place in the BI system.

An early use of the phrase that Snowden “slipped through the cracks” appears in a *New York Times* report where an unnamed law enforcement official commented that Snowden and his previous attempts to obtain unauthorized classified information had “slipped through the cracks,” due to others failing to recognize the importance of a 2009 derogatory CIA employment report on Snowden (Schmitt 2013). According to the newspaper, Snowden’s supervisor at the CIA in 2009 wrote in his employment file that “Snowden was trying to break into classified computer files to which he was not authorized to have access,” so he was sent home from Geneva. The CIA failed to submit this to the NSA or its contractors, so thus, “the red flags went unheeded,” and his report “slipped through the cracks.”

The US Senate also employed the basic premise this phrase that Snowden had somehow slipped through a normally infallible system. In June 2013, eleven days after Snowden’s disclosures, Congress met to interrogate the security clearance process and national security programs (US Senate, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Subcommittee on Financial and Contracting Oversight 2013). In the opening statements of the discussion, Senator Jon Tester posed the question, that after so much effort to screen those with access to classified information through BIs, “How in the world does a contractor, who had been on the job for less than 3 months, get his hands on information detailing a highly classified Government program that he subsequently shared with foreign media outlets?” (2013: 1-2). He went on to suggest that there was a problem in the overall security clearance procedure, and in another hearing in November he also commented that it only takes one person to “slip through the cracks” (US Senate, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Committee on Homeland Security and Governmental Affairs 2013: 2). Senator Rob Portman described similar sentiments when he testified that Snowden’s BI demonstrated “the inadequacy of the system” (US Senate, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Subcommittee on Financial and Contracting Oversight 2013: 4). Additionally, because events such as Snowden’s unauthorized disclosures of information, Tester continued that “it is abundantly clear to the American people that the Federal Government is failing to properly vet the individuals who are granted access to our nation’s most sensitive information and secure facilities” (US Senate, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Committee on Homeland Security and Governmental Affairs 2013: 1).

The investigations into the BI program caught even more steam by September when another contractor named Aaron Alexis was also positioned to have slipped through the cracks. Alexis used his clearance, not to disclose classified information like Snowden, but to gain access to a facility where he murdered twelve people before he was killed by security (USHRCOGR 2014b: 2). Because Alexis’ acts took place so close to Snowden’s disclosures, both were subsequently intertwined as examples of the failures of the BI process. In November 2013, Committee on Oversight and Government Reform chairman Darrell Issa wrote in a letter to OPM that Congress needed to do everything possible about BIs because, although the cases of Snowden and Alexis had different circumstances, the “the security clearances that both Snowden and Alexis received from the federal government allowed them to carry out their heinous acts” (US House

of Representatives 2013: 1). He continued that as based off information developed from an analysis of both cases, the BI process has “major gaps” and the problems needed to be fixed.

In February 2014, the federal government released a report after a study of Alexis’s case narrating several flaws overall in the BI process. These flaws are constructed to be reasons for the failures of the BI process. They are contextualized in the larger argument of Snowden because Snowden’s actions initially triggered the investigation into the BI (US Senate, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Subcommittee on Financial and Contracting Oversight 2013: 2). Among several conclusions, key findings of this report included that in BIs, there is a “non-cooperation of 450 police departments with federal background investigators;” “lack of continuous monitoring;” and that “regulations prohibit background checkers from looking at the Internet or social media when performing checks” (USHRCOGR 2014a). Looking specifically at these three areas, it is interesting to note that within this narrative of how the BI process is flawed exists a counter-narrative which shows that although Snowden revealed an extent of how much the government is collecting, at the same time, the flaws of the BI process also show how the government is in some ways limited in its data collection of the very people that are supposed to be in charge of classified information.

Regarding these flaws, first there was a lack of cooperation with law enforcement agencies (USHRCOGR 2014b: 16; USHRCOGR 2014a). Law enforcement screening would seem to be routine for applicants for security clearances as well as for other more basic checks for non-confidential employment. It has been studied that government employees “are the targets of intensive police screening” (Ericson and Haggerty 1997: 237). Apparently, though, when it comes to background investigations, 450 law enforcement agencies aren’t cooperating with OPM (USHRCOGR 2014b: 3). Many of the organizations that do not cooperate are large metropolitan agencies such as the police departments of Los Angeles, New York, Newark, and Washington, D.C. (2014b: 42). The report shows that Newark’s reason they won’t provide information is because they only cooperate with other law enforcement agencies (despite that OPM is supposed to have agreements with law enforcement institutions as established by multiple executive orders, laws, and regulations) (2014b: 16), and another example in an unnamed agency shows that “staff told [an] agent it was ‘illegal’ for her to request records and threatened her with arrest if she returned” (2014b: 17). Apparently, OPM can’t obtain this information because it is limited by a lack of an “enforcement mechanism against local law enforcement agencies that refuse to comply” (2014b: 40). This is interesting because as Lyon discusses, many assume that “surveillance systems are all-powerful” (Lyon 2007: 82) but in this case, the OPM BIs are failing to get cooperation from law enforcement agencies. Instead, this surveillance system is more accurately “contingent, fluid, and unpredictable” because not every agency complies with OPM and its policies.

Second, the report suggested there was a need to have continuous evaluations during the duration of clearances (USHRCOGR 2014a). The current BI process does require some evaluations depending on the different level of clearances: an individual with a TS clearance needs a new investigation after five years. This time moves to ten years for a Secret clearance and fifteen for a Confidential (USHRCOGR 2014b: 32). While this may seem to mean continuous monitoring, within the five, ten, and fifteen year periods, OPM is not tasked with doing any other observations or surveillance except when the employee meets those time markers. During these gaps, the person with the clearance is supposed to self-report misconduct between the investigations, but otherwise, “there is no mechanism” to determine if misconduct is actually being reported (2014b: 11). This is interesting in light of other data provided by the GAO showing that many times problems like tax debt occur after BIs are conducted, and “approximately 6,300 individuals (about 76 per cent) amassed tax debts after their clearances were issued” (GAO 2013: 16). Tax debt, according to the risk definitions of the BI, is a consideration for the adjudication process.

The third flaw detailed that background investigators are “strictly prohibited” (USHRCOGR 2014b: 36) from using the internet or social media sites. Investigations cannot incorporate internet information, and

any leads obtained using the internet are not admissible in reports. Leads can only be of the general type such as “to locate the address of the facility or the homepage of a government office to locate points of contact” (2014b: 3). Leads cannot be information on subjects of investigation to include a subject’s identifiers. The report concludes that OPM’s policies are outdated and should be forced “into the twenty-first century.”

It is interesting to learn that the government doesn’t use the internet to search for information when vetting candidates, especially as Lyon points out, that after 9/11, “the internet came into its own as a means of running security screens on job applicants” (2007: 42). Merton Miller, Associate Director of OPM, defended the agency and its policies and commented that using the internet in BIs is problematic because of privacy concerns and the reliability of online communication. Miller questioned if any analytics could ever efficiently verify any of the information written on the internet and argued that an accurate analysis of the information would be very difficult. Miller came to the conclusion that without knowing the validity of information, one “shouldn’t be incorporating information that isn’t true about the subject in that investigation” (USHRCOGR 2014b: 38). This statement butting up against other anecdotal news stories about children being visited by the Secret Service due to what they wrote on the internet (Fox News Network 2011) is intriguing. In other cases, online information can be construed as a credible threat, but for BIs, online information is not reliable enough.

Analysis

These calls for reform are important to analyze for four reasons. First, put together, the US government is constructing these points in a narrative as to why BIs are insufficient. Each of these points shows how the BI process is not achieving its goals and is thus allowing some to slip through the cracks. These gaps are places where the government implies that not enough information is being gathered. So while much of the coverage on Snowden is focused on debating how to reduce the information the government obtains, when it comes to BIs, Snowden started a conversation in government that ultimately ended with government deciding that not enough information is being obtained. To avoid more disclosures, Congress’ narrative has triggered calls for reform to broaden the scope of government and obtain more information.

Second, calls for reform highlight Snowden’s effects on government employees on concerns such as privacy and whistleblowing abilities in several ways. First, as previously discussed, the 2009 CIA potentially derogatory employment file was not shared with the NSA. According to *The New York Times* article, the CIA and NSA used an electronic system to monitor security clearances but they had previously not monitored more than “major rule-based infractions” and not behavioral problems, so this information was not known to the NSA (Schmitt 2013). However, since Snowden, “that flaw has since been corrected and such information is now being pushed forward.” Whether or not this is a good or bad thing can be debated, but in this case it does show that employees have less privacy and more information is being shared between agencies.

Additionally, in a post-Snowden open hearing on security clearance reform, Brian A. Prioletti from the Office of the Director of National Intelligence indicates that due in part to Snowden, continuous monitoring is now a high priority for the BI process. In order to fix this, the government is working on several things, and among them, one is to incorporate the Continuous Evaluation (CE) tool which has the intentions to include more “automated records checks of commercial databases, government databases, and other information lawfully available” (US Senate, Committee on Homeland Security and Governmental Affairs 2013: 4-5) because “manual checks are inefficient and resource intensive” (2013: 5). The CE program supports Insider Threat Programs which are designed to keep track of those that have disclosed classified information or were involved with workplace violence. In this way, the government illustrates principles of the control society by becoming more comprehensive and reliant on technological databases in hopes of continual evaluation.

Additionally, according to Prioletti, ODNI and OPM are also working on a position designation process to standardize how security positions are classified. Prioletti affirms, “The Federal workforce will benefit from accurately designated positions” (US Senate, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Committee on Homeland Security and Governmental Affairs 2013: 6), but not everyone agrees. While this uniformity will seemingly help agencies designate clearance levels appropriately, there has already been pushback. Some think that this rule will harm certain segments of the population. Senator Jon Tester issued a statement in conjunction with Ranking Member Rob Portman in response to this proposal. He testified that “far too many questions remain unanswered about the implications of this proposal” (2013: 2). Additionally, David Borer, General Counsel for the American Federation of Government Employees comments that this proposal will allow “agencies to pick and choose which employees will have the right to due process before the MSPB” (2013: 10). Borer points out that “these new rules fail to direct the agencies that in order to designate a national security position, they must make an affirmative determination that the occupant of that position could cause a material, adverse effect on national security through neglect, action, or inaction” (2013: 11). Angela Canterbury seems to think this new proposal intends not necessarily to limit clearances to more appropriate designations, but rather to “expand the use of these designations to overly-broad categories” (2013: 12).

For Borer and Canterbury, these proposed changes are especially concerning because of *Kaplan v. Conyers*, a post-Snowden court ruling from August 2013 which, according to Canterbury, eliminates “civil service due process rights and whistleblower protections for anyone in a national security sensitive position” (Canterbury 2013: 4). The US Office of Special Counsel echoed these sentiments and stated that they were disappointed in the ruling. The office issued a statement saying, “This decision poses a significant threat to whistleblower protections for hundreds of thousands of federal employees in sensitive positions and may chill civil servants from blowing the whistle” (US Office of Special Counsel 2013).

Third, the premises that Snowden slipped through the cracks is questionable since the phrase engenders ideas of a fairly dependable system through which he could “slip through the cracks.” “Slipping through the cracks” implies that there may be some things to fix, but these problems can be addressed and the system can go back to functioning fairly well. Looking at the history of BIs though shows a history of problems that didn’t just start with Snowden. In the 1950s and 1960s, due to perceived Cold War fears, the US government set about establishing permanent security and protection procedures (Defense Personnel Security Research Center [DPSRC] 2005: A-14). OPM specifically traces their authority to conduct background investigations for security clearances back to the Executive Order (E.O.) 10450 or the “Security Requirements for Government Employment” issued in April 1953 (USOPM 2015b). This order gave OPM the authority to conduct background investigations to determine risk on government employees. OPM also indicates that over the years, there have been several updates to this order; however, in the 63 years since the initial authority was granted, there have only been six additional executive orders issued. The first two updates, E.O. 12958 and 12968, were both issued in 1995. E.O. 12958 redefined how classified information was identified, protected, and declassified, and E.O. 12968 established a uniform personnel security program for access to classified information. The next order, E.O. 13381, was issued ten years later in 2005 and strengthened the process for determining eligibility for classified information. The fourth update, E.O. 13467, was issued in 2008 and was designed to reform the clearance process for government employees and contractors and their ability to access national security information. The fifth and sixth orders, 13488 and 13526 were both issued in 2009. E.O. 13488 and E.O. 13526 use similar verbiage as E.O. 12968 (classifying, safeguarding, and declassifying) but adds an additional element to the declassification element and by including information about terrorism.

The E.O.s listed on OPM’s website do not fully reveal the turmoil that has continually boiled under the surface of the security clearance process, however. In a report by the Defense Personnel Security Research Center, Eric L. Lang traces the history of the background investigation / security clearance program and

outlines a record of ongoing attempts to reform the security clearance process. While the 1950s and 1960s saw legislation to establish permanent security procedures, the 1970s and 1980s, due to a perceived increase in espionage cases or the “espionage plague” (to which Lang attributes to the change in prosecution rather than an actual increase in cases), saw calls for reform for these procedures (DPSRC 2005: A-15). By 1985, a report by the Stillwell Commission criticized the number of security clearances being issued, and going on recommendations from this report, in 1991, National Security Directive 63 was issued which further established investigation standards and program consolidations (A-16). By 1993 though, many of the problems identified by the Stillwell report still existed, and due to this, the Joint Security Commission was created which pushed for more reform such as the implementation of periodic reinvestigations which continues to monitor employees with access to secure information. By 1994, the security community was in a Snowden-esque uproar upon the discovery of espionage created by Aldrich Ames, and this prompted more reform such as requiring financial disclosures for those holding clearances (A-17). By 1996, arguments about the costs of the processes came to a head, and OPM privatized its investigative employees and turned its investigative branch into an Employee Stock Owned Plan and company called USIS (Barr 1996: A19). Lang reports that personnel clearance reform hit a low point by October 1999 when the GAO found that 92 per cent of Defense Security Service (DSS) (another service conducting background investigation mostly for the Department of Defense) investigations lacked required data, and due to new reinvestigation requirements, background investigations were taking longer which resulted in backlogs (DPSRC 2005: A-18). By 2001, there was still criticism of DSS’s inadequate reports and backlogs, and by 2004, 1,800 of the DSS staff went to OPM (USOPM 2004) for OPM to now conduct all of the Department of Defense’s BIs. Despite the consolidation, there were still many troubles. In 2008 and 2009, timeliness and quality issues resurfaced again (GAO 2008; GAO 2009). In 2010, there were concerns of privacy, and OPM was criticized for how it was handling personal identifiable information (GAO 2010). In 2012, OPM was involved in transparency issues over the costs of BIs (GAO 2012). So by the time Snowden came around a year later in 2013, OPM and the BI/security clearance had already been continually going through turmoil. A belief in an idea that Snowden “slipped through the cracks” seems to be a stretch when compared to a history of program problems.

Fourth, the conversation perpetuates a myth of the “whole person” which helps explain why calls for more surveillance are flourishing. As Lyon comments, it is not good enough to know where surveillance is happening, but we also need to know why it is proliferating (Lyon 2007: 2). Underpinning the investigation and adjudication practices in BIs is the idea of the whole person. It proliferates in the discourse of many discussions of the final determination of clearances. For instance, OPM’s site asserts that adjudicators use the “whole person” for evaluation and determination of clearances which means “[a]ny potentially negative information is evaluated regarding its recency, seriousness, relevance to the position and duties, and in light of and in relationship to all other information about a person” (USOPM 2015c). This belief then implies that the information gathered will be able to provide an accurate and complete picture of who a security clearance applicant really is.

While it may appear generous of the government to look at the “whole picture” of an individual rather than an isolated incident, really, it is problematic that the US government claims to assemble data which would provide a “whole picture” of a person. For starters, the whole idea of identity is theoretically challenged. Identification can be seen as an act of the powerful through bureaucratic or state-defined characteristics, and this can be seen through the difference between the concept of identity and identification (Caplan and Torpey 2001). According to Lyon (2009), the difference between the two words is that *identification* is a remote form of classification where individuals are grouped through institutional constraints, and *identity* is a more personal self-expression of who one thinks they are. Differentiating between the two is important then because identification, which the BI does, is imposed from the outside, and identity is a more self-constructed idea composed by a person about him or herself. The “whole person” idea aligns with identification and is a collection of data points that US government uses in deciding what makes up a person, but it isn’t necessarily who individual under investigation thinks that

they are. For instance, the SF-86 form asks about prior alcohol or drug treatment (USOPM 2015d), and the government uses this information during the adjudication process (US Department of State 2006). This can be problematic because an individual that has overcome his/her alcohol or drinking problem may no longer feel that this treatment defines him/her, but it is still considered part of the “whole person” identification and could affect the clearance granting.

Also, upon closer look of this phrase, the possibility of really capturing the “whole person” through a set of institutional requirements and limitations is a stretch. The “whole person” functions really more as a synecdoche where parts are representative of a whole rather than an actual “whole person” (Wise, Goggin, and Rose 2016). The BI gathers specific institutionally-defined information about an applicant that supposedly stands for the whole person; however, that whole is only reflective of a limited amount of information required to be gathered by an investigator as dictated from the SF-86 (USOPM 2015d) and as available to be obtained. The US Department of State almost seems to acknowledge this when it says adjudication using the whole person concept means using “[a]vailable, reliable information about the person, past and present, favorable and unfavorable” to determine suitability (US Department of State 2006). By using the word “available,” the agency implies that the “whole person” is made of only available information, and when it adds “reliable,” it doesn’t give criteria of the determination of reliable. However, unavailable information would still be representative of a “whole,” and reliable criteria could be information from a law enforcement agency but erroneously entered under the wrong person’s name and really shouldn’t be considered part of a “whole.” The “whole” then is really only a collection of a few parts and what was able to be obtained at a certain time in a certain set of circumstances. The “whole” is only a sum of limitations and not really a “whole person.”

Additionally, even in the earlier discussion of recommendations for fixing the clearance process, the government acknowledged investigators can’t use information from internet sources. For a wired society, it seems counterintuitive to consider a “whole person” without taking into account online activities. Although the Consolidated Appropriations Act of 2016 mandates “the Office of the Director of National Intelligence direct federal agencies to adopt a personnel security program integrating social media information by the end of 2020” (USHRCOGR 2016), this measure is not a current practice and shows BIs are thus dictated by rules prescribed by handbooks and not necessarily real iterations of a “whole person.”

So thus, despite attempts to obtain a complete and whole picture of a person, a BI produces not a whole person, but just a whole person myth; one has only gathered an assemblage of some portions of data. It draws upon the conflation between the terms identity and identification, and it assumes that an outside institution is able to identify the character of an individual so much that it can predict future actions. Edward Snowden supposedly slipped through the cracks because the BI failed to predict the future by failing to accurately assess background information based on his “whole person.” But instead of acknowledging that maybe the future can’t be predicted and identity is constructed and transient at best, blame was placed on deficient BI processes. This further allows for calls for more surveillance to proliferate.

Conclusion

In a constructionist approach, risks exist, but they are socially and politically influenced. Paying attention to how those risks are constructed helps identify the reasons surveillance proliferates. The US government defines risks for classified information through the investigative and adjudicative processes; the rules that dictate these processes also define what a risk is and what information should be gathered. Snowden’s obtaining a clearance came to represent the epitome of failure of the BI. Because Snowden divulged classified information, he must have slipped through the cracks of the BI process. Thus, more information should be gathered to fill in the gaps.

Overall, the example of the BI offers a counter-narrative to the narrative typically attributed to Snowden. Instead of seeing how wide-spread the US government's surveillance capabilities are, the BI shows how limited the US government is in some capabilities and the "failure" of current surveillance tactics. The government's use of the construct "slipping through the cracks" and similar phrases has caused a call for more surveillance—exactly what Snowden wanted to avoid. While these calls for more surveillance aren't surprising especially in light of information that Snowden revealed, they should be paid attention to. The conversation of the BI has implications in calls for more surveillance, privacy and whistleblowing capabilities, belief that an infallible system exists, and the belief that the BI can actually capture the essence of an individual so much that it can tell the future. All of these elements are problematic and each point can be used to justify more surveillance and helps show how surveillance proliferates in modern society.

References

- Andrejevic, Mark. 2006. "The Discipline of Watching: Detection, Risk, and Lateral Surveillance." *Critical Studies in Media Communication* 23(5): 391-407.
- Barr, Stephen. 1996. "Long-Term OPM Savings to Cost \$5.7 Million Now." *The Washington Post*, May 22. ProQuest (1033969862).
- Beck, Ulrich. 1992. *Risk society: Towards a New Modernity* (M. Ritter, Trans.). London: Sage.
- Brickley, Peg. 2015. "Altegrity Files for Chapter 11 Bankruptcy: Company Gained Attention After Vetting Former NSA Contractor Edward Snowden." *Wall Street Journal*. Feb. 8. Accessed April 27, 2015. <http://www.wsj.com/articles/altegrity-files-for-chapter-11-bankruptcy-1423446150>.
- Canterbury, Angela. 2013. "Canterbury's Senate Testimony on National Security Positions." Project on Government Oversight. Accessed June 7, 2014. <http://www.pogo.org/our-work/testimony/2013/canterburys-senate-testimony-on-national-security-positions.html>.
- Caplan, Jane, and John Torpey. 2001. "Introduction." In *Documenting Individual Identity*, eds. Jane Caplan and John Torpey, 1-12. Princeton, NJ: Princeton University Press.
- Castel, Robert. 1991. "From Dangerousness to Risk." In *The Foucault Effect: Studies in Governmentality: With Two Lectures by and an Interview with Michel Foucault*, eds. Graham Burchell, Colin Gordon, and Peter Miller, 281-298. Chicago: University of Chicago Press.
- Defense Personnel Security Research Center [DPSRC]. 2005. *Security Background Investigations and Clearance Procedures of the Federal Government*, by Eric L. Lang. Monterey, CA: Defense Personnel Security Research Center. <http://www.dhra.mil/perserec/reports/mr05-05.pdf>.
- Deleuze, Gilles. 1992. "Postscript on the Societies of Control." *October* 59: 1-7.
- Ekberg, Merryn. 2007. "The Parameters of the Risk Society: A Review and Exploration." *Current Sociology* 55(3): 343-366.
- Ericson, Richard V., and Kevin D. Haggerty. 1997. *Policing the Risk Society*. Toronto: University of Toronto Press.
- Fox, Nick J. 1999. "Postmodern Reflections on "Risk", "Hazards", and Life Choices." In *Risk and Sociocultural Theory: New Directions and Perspectives*, ed. Deborah Lupton, 12-33. Cambridge: Cambridge University Press.
- Fox News Network. 2011. "13-Year-Old Boy Questioned by Secret Service Over Facebook Posting." *Fox News*. Accessed June 1, 2014. <http://www.foxnews.com/us/2011/05/17/13-year-old-boy-questioned-secret-service-facebook-posting/>.
- Gandy, Oscar H. Jr. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press.
- Giddens, Anthony. 1999. "Risk and Responsibility." *The Modern Law Review* 62(1): 1-10.
- Gilliom, John, and Torin Monahan. 2013. *SuperVision: An Introduction to the Surveillance Society*. Chicago: University of Chicago Press.
- Government Accountability Office [GAO]. 1999. "Inadequate Personnel Security Investigations Pose National Security Risks." Report to the Ranking Minority Member, Committee of Armed Services. House of Representatives 05-552: 1-67.
- Government Accountability Office [GAO]. 2000. "Inadequate Personnel Security Investigations Pose National Security Risks." Testimony Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives T-NSIAD-00-65: 1-13.
- Government Accountability Office [GAO]. 2008. "Personnel Clearances: Key Factors to Consider in Efforts to Reform Security Clearance Processes." Testimony Before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, House of Representatives GAO-08-352T: 1-17.
- Government Accountability Office [GAO]. 2009. "Personnel Security Clearances: An Outcome-Focused Strategy and Comprehensive Reporting of Timeliness and Quality Would Provide Greater Visibility over the Clearance Process." Testimony Before the Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, House of Representatives GAO-10-117T: 1-13.
- Government Accountability Office [GAO]. 2010. "Privacy: OPM Should Better Monitor Implementation of Privacy-Related Policies and Procedures for Background Investigations." Report to the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate GAO-10-849: 1-30.

- Government Accountability Office [GAO]. 2012. "Background Investigations: Office of Personnel Management Needs to Improve Transparency of Its Pricing and Seek Cost Savings." Report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate GAO-12-197: 1-67.
- Government Accountability Office [GAO]. 2013. "Security Clearances: Additional Mechanisms May Aid Federal Tax-Debt Detection." Report to Congressional Requesters. 13-733: 1-48.
- Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. 2013. "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations." *The Guardian*, June 11. Accessed April 27, 2015. <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. "The Surveillant Assemblage." *British Journal of Sociology* 51(4): 605-22.
- Hakamaa, Marko. 2016. "New Clearance Data System Ready for Roll-Out." *Clearance Jobs.com*. Accessed October 30, 2016. <https://news.clearancejobs.com/2016/06/23/new-clearance-data-system-ready-roll/>.
- Jenkins, Richard. 2012. "Identity, Surveillance and Modernity: Sorting Out Who's Who." In *Routledge Handbook of Surveillance Studies*, eds. Kirstie S. Ball, Kevin D. Haggerty, and David Lyon, 159-166. Oxon: Routledge.
- Loveridge, William. 2012. "What is JPAS (Joint Personnel Adjudication System)?" *Clearance Jobs.com*. Accessed October 30, 2016. <https://news.clearancejobs.com/2012/08/06/what-is-jpas-joint-personnel-adjudication-system/>.
- Lupton, Deborah. 1999. *Risk*. New York: Routledge.
- Lyon, David. 2003. "Surveillance as Social Sorting: Computer Codes and Mobile Bodies." In *Surveillance as Social Sorting: Privacy, risk and Digital Discrimination*, ed. David Lyon, 13-30. New York: Routledge.
- Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity.
- Lyon, David. 2009. *Identifying Citizens: ID Cards as Surveillance*. Malden: Polity.
- Marwick, Alice E. 2012. "The Public Domain: Social Surveillance in Everyday Life." *Surveillance & Society* 9(4): 378-93.
- Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley, CA: University of California Press.
- Nadesan, Majia. H. 2008. *Governmentality, Biopower, and Everyday Life*. Florence: Routledge.
- Office of the White House. 2014 "Suitability and Security Process Review Report." Report to the President. Last modified February 2014. <https://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf>.
- Scheuerman, William E. 2014. "Whistleblowing as Civil Disobedience: The Case of Edward Snowden." *Philosophy and Social Criticism* 40(7): 609-628.
- Schmitt, Eric. 2013. "C.I.A. Warning on Snowden in '09 Said to Slip Through the Cracks." *The New York Times*. Accessed June 7, 2014. http://www.nytimes.com/2013/10/11/us/cia-warning-on-snowden-in-09-said-to-slip-through-the-cracks.html?_r=0.
- Staples, William G. 2000. *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowman & Littlefield Publishers, Inc.
- US Department of State. 2006. "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information." Feb. 3. Accessed April 27, 2015. <http://www.state.gov/m/ds/clearances/60321.htm>.
- US House of Representatives. 2013. "Letter - Committee on Oversight & Government Reform." Accessed June 6, 2014. <http://oversight.house.gov/wp-content/uploads/2013/11/2013-11-20-DEI-to-Archuleta-re-in-camera-review-due-11-21-13.pdf>.
- US House of Representatives. Committee on Oversight and Government Reform [USHRCOGR]. 2014a. "Report: D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process." Accessed May 15. <http://oversight.house.gov/release/report-d-c-navy-yard-shooting-exposes-flaws-federal-security-clearance-process>.
- US House of Representatives. Committee on Oversight and Government Reform [USHRCOGR]. 2014b. *Slipping Through the Cracks: How the D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process*. 113th Cong, 1st Sess., February 11.
- US House of Representatives. Committee on Oversight and Government Reform [USHRCOGR]. 2016. "Incorporating Social Media into Federal Background Investigations." Accessed October 29. <https://oversight.house.gov/hearing/incorporating-social-media-federal-background-investigations/>.
- US Office of Personnel Management [USOPM]. 2004. "OPM Consolidates Bulk of Federal Security Clearance Process with Transfer of Over 1,800 Employees from Defense Department Vast Majority of Federal Background Investigations to be Centered at OPM." Nov. 22. Accessed April 21, 2015. <https://www.opm.gov/news/releases/2004/11/opm-consolidates-bulk-of-federal-security-clearance-process-with-transfer-of-over-1800-employees-from-defense-department/>.
- US Office of Personnel Management [USOPM]. 2015a. "Background Investigations." Accessed April 30. <http://www.opm.gov/investigations/background-investigations/>.
- US Office of Personnel Management. 2015b. "Background Investigations: Reference Materials." Accessed April 20. <http://www.opm.gov/investigations/background-investigations/reference/general/#url=Executive-Orders>.
- US Office of Personnel Management. 2015c. "Frequently Asked Questions: Investigations." Accessed April 27. <http://www.opm.gov/faqs/QA.aspx?fid=cb3cafac-1e73-4a6b-bd88-a3adad355390&pid=922beea7-1b14-4b22-92e6-be305d5d1d6e>.
- US Office of Personnel Management. 2015d. "Questionnaire for National Security Positions." Accessed April 27. http://www.opm.gov/Forms/pdf_fill/sf86.pdf.

- US Office of Personnel Management. 2016. "National Background Investigations Bureau." Accessed October 29. <https://nbib.opm.gov/>.
- US Office of Special Counsel. 2013. "Statement in Response to Ruling on Kaplan v. Conyers." Last modified August 21. https://osc.gov/News/pr13_06.pdf.
- US Senate. Committee on Homeland Security and Governmental Affairs. 2013. "Open Hearing on Security Clearance Reform by Brian Prioletti." Statement for the Record. October 31. <http://www.dni.gov/index.php/newsroom/testimonies/194-congressional-testimonies-2013/958-statement-for-the-record.-open-hearing-on-security-clearance-reform>.
- US Senate. Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Committee on Homeland Security and Governmental Affairs. 2013. *Safeguarding Our Nation's Secrets: Examining the National Security Workforce*. 113th Cong, 1st Sess., November 20.
- US Senate. Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, Subcommittee on Financial and Contracting Oversight, Committee on Homeland Security and Governmental Affairs. 2013. *Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*. 113th Cong, 1st Sess., June 20.
- Wise, J. Macgregor, Peter Goggin, and Shirley Rose. 2016. In-person dissertation defense with Sarah Young. September 16. Arizona State University. Tempe: AZ.
- Young, Sarah J. 2015. "Literacies for Surveillance: Social Network Sites and Background Investigations." *Media and Communication* 3(2): 88-97.