pre-print contribution to Akhgar et al. *Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, 1st edn. Butterworth-Heinemann, 2015.

CHAPTER FIVE

Interpretation and Insider Threat: Re-reading the Anthrax Mailings of 2001 Through a "Big Data" Lens

Bethany Nowviskie, Ph.D. and Gregory B. Saathoff, M.D.
University of Virginia

In the wake of the notorious anthrax mailings of September and October 2001, investigators lacked computational tools and digitized information sources more readily available today through modern bioinformatics and in the form of comparative social, linguistic, and behavioral datasets.[1] Nor did the common fund of knowledge required to apply so-called "big data" analysis to behavioral science allow such techniques to be employed beyond a rudimentary fashion. The United States Federal Bureau of Investigation (FBI) led an extensive and costly investigation into the identity of the mailer through the years that followed the attacks, with the assistance of the United States Postal Inspection Service. By 2007, the Department of Justice (DOJ) had determined that "the single spore-batch [of *Bacillus anthracis*] created and maintained by Dr. Bruce E. Ivins at the United States Army Medical Research Institute of Infectious Diseases ("USAMRIID") was the parent material for the letter spores."(2010). Dr. Ivins remained under investigation for these crimes both before and after his death by suicide in the summer of 2008.

Ivins worked in an extremely dangerous arena and—like other such researchers—as a condition of his employment, he assented to certain safeguards and active monitoring in the form of data collection. These safeguards were designed to protect the public from what has been called "insider risk" or "insider threat "(Shaw *et al.,* 2009; Silowash *et al.*, 2012). Therefore, Dr. Ivins did not retain the privacy protections held by civilian employees in most workplaces, either private or governmental. Because he worked in a top secret environment with biological select agents or toxins (BSATs) including anthrax, Ivins was also required to waive confidentiality of his medical and mental health records.

[1] One of the outcomes of this case was the development & advancement of modern bioinformatics by The Institute for Genomic Research (TIGR)

Despite this waiver, Ivins' mental health records were not ever examined by federal investigators during his lifetime, and do not appear to have been accessed prior to his hiring. Notably, they contained admission of crimes that would have precluded his employment and security clearance had this information come to light. Like the information collected on Ivins' communications and on his comings and goings in the workplace, his mental health records did prove to be illuminating after a formal, post-mortem review was authorized by Chief Judge Royce Lamberth of the United States District Court of Washington, D.C.[2]

Although examination of the "Amerithrax" case could provide insight into the potential for *prediction* of bioterror incidents perpetrated by insiders, predictive uses of big data analysis (with all of their attendant concerns for privacy and civil liberties) are not a focus of this chapter. Nor is this a chapter on current best practices in deterring insider threat, or a how-to in applying particular data analysis techniques. In fact, the Report of the Expert Behavioral Analysis Panel (EBAP), a non-governmental independent panel of medical and systems experts, did not initiate or utilize data mining in its 2009-2010 review of relevant material. Rather, we will examine this historic case conceptually—particularly by tracing the retrospective inquiry into available records conducted by the Lamberth-authorized EBAP from July 2009-August 2010. We do this in the context of current data mining techniques, available corpora for analysis, understandings of the relationship between algorithm and interpretation (Nowviskie 2014; Nowviskie 2014a), and ethical conversations surrounding big data.

Effective application of big data analysis could potentially augment the ability of investigators to solve difficult crimes involving insider threat. But insider threat cases also pose an opportunity to reflect on important ethical and interpretive facets of computational text analysis and data mining. These range from judgments made during

[2] The review was commissioned in July 2009 and chaired by one of the current chapter's co-authors. It issued its report, *The Amerithrax Case: Report of the Expert Behavioral Analysis Panel*, in August of 2010. Although initially sealed, a redacted version was released in March of 2011 through Federal Court order of Judge Lamberth. Any material cited in this chapter remains publicly available. No information provided in this chapter reflects Grand Jury material or still-undisclosed or privileged information that is protected through patient privacy law (HIPAA).

the selection, collection, and disclosure of data, to the considered choice of algorithmic tools to aid in discovery, visualization, and expert interpretation by behavioral analysts. It is important for law enforcement investigators to understand that big data analysis in crime-solving and behavioral analysis is rife with decision-making and contingency. Its conclusions can be dependent upon the subjective standing points of those who assemble data sets, design the processes by which they are analyzed, and interpret the results. In other words, such techniques provide no push-button answers—only arrangements of information that must be interpreted in almost a literary sense and which, in fact, themselves depend on a chain of previous decision-points, interdependencies, moments of expert intuition, and close, interpretive readings (Chessick, 1990). It is little wonder, then, that many of our citations for this chapter come from the academic field of the digital humanities. Scholars in the field have grappled with the relationship of algorithmic toolsets and data visualization techniques to the making of meaning, and to deeply subjective, interpretive, and ethical questions in disciplines like history, literature, and anthropology for decades (Gold, 2012). Data mining is an aid to interpretation of selected and processed (therefore, in some sense, *pre*-interpreted) datasets. It can be a crucial means of focusing investigators' attention—but is never a substitute for close and critical reading of sources, or for psychological and behavioral analysis. That is the key lesson to be taken from this chapter.

Importance of the Case

This was the longest and most expensive investigation ever undertaken by the FBI. It began in 2001, in the wake of the September 11th jet airliner attacks on the World Trade Center in New York City and on the Pentagon in Washington, D.C. Only one week after these dramatic and visually striking airliner attacks, a stealthy, unwitnessed attack was perpetrated in the form of anthrax-laden letters, postmarked after having been picked up from a mailbox in Princeton N.J. The "ensuing criminal investigation," according to the Department of Justice (DOJ) Report (2010):

> "was extraordinarily complex, given the possible breadth and scope of this bioterrorism attack. In the seven years following the attack, the Amerithrax Task Force expended over 600,000 investigator work hours, involving in excess of

> 10,000 witness interviews conducted on six continents, the execution of 80 searches, and the recovery of over 6,000 items of potential evidence. The case involved the issuance of over 5,750 federal grand jury subpoenas and the collection of 5,730 environmental samples from 60 site locations. Several overseas site locations also were examined for relevant evidence with the cooperation of the respective host governments."

The human toll of the anthrax mailings included citizens in the private sector and government, resulting in five deaths due to inhalational anthrax and direct infections occurring in at least seventeen others.

But the impact on individual citizens included more victims than those who either died of anthrax or suffered bacterial infection. Thousands of possibly exposed, but symptom-less individuals were treated with antibiotics as a public safeguard. Postal workers experienced a dramatic evolution and devolution of the U.S. Postal Service. Policies and procedures relating to national security were modified, affecting scientists and laboratories in the academic, governmental and private sectors. In the course of the investigation, one later-exonerated scientist who had been named early on as a "person of interest" ultimately received a 4.6 million dollar settlement from the U.S. government (Lichtblau, 2008). Because the anthrax used in the crime had originated at USAMRIID, scientists who worked there at Fort Dietrich experienced the stress of an ongoing federal investigation that occurred over the course of several years.

Finally, and perhaps most critically, concerns about the potential for bioterrorism raised by these incidents fed into the passage of the now-controversial USA PATRIOT Act and formed a key part of the justification for the US invasion of Iraq. The spectre of the anthrax mailings was raised dramatically in a February 2003 speech to the United Nations Security Council, when former Secretary of State Colin Powell shared since-discredited intelligence as to Iraq's biological weapons capability. While suggesting that the Saddam Hussein regime may have produced up to 25,000 liters of anthrax able to be distributed from spray tanks on unmanned drones, Powell brandished a prop vial to remind his audience that “less than a teaspoon full of dry anthrax in an envelope shutdown the United States Senate in the fall of 2001.”(CNN: Cable News Network, 2003) (Weisman, 2005). Prior to this, the PATRIOT Act, signed into law by then-President George W. Bush in October of 2001 and since repeatedly contested by civil liberties advocates, had dramatically expanded the ability of government agencies to collect and demand disclosure of information useful for big-data pattern analysis of the activities of both private US citizens and foreign nationals. And researchers have noted a clear “chilling effect” on the day-to-day information-seeking behavior of average citizens—such as Google users apparently reluctant to conduct innocent searches for words like “anthrax”—in the months following the July 2013 revelations by Edward Snowden of improper government surveillance (Pasternack, 2014). Thus the Ivins case sits squarely at a crucial nexus of personal, social, ethical, and historical consequences for both insider threat and bioterror prevention, and for the use of big data in law enforcement.

The Advancement of “Big Data” Analytics After 2001

Although the FBI’s 2001 investigation involved, in part, the review of 26,000 e-mails, the analysis of 4 million megabytes of data in computer memory, and information collected from 10,000 witness interviews and 5,750 grand jury subpoenas, the ready availability of truly astronomical amounts of digitized and born-digital information to law enforcement and academic research is a recent phenomenon (FBI 2011). The legal landscape for surveillance and subpoena of digital data by the government expanded rapidly, though not without later controversy and critique, under the USA PATRIOT Act of 2003. Commerce-driven analytic techniques that are commonplace now were not as regularly utilized at the turn of the last century, in part due to the dearth of available consumer data. And mass digitization of the historical and contemporary print record under projects such as Google Books had just begun. Indeed, by some estimates, 90% of the world’s actionable cultural data has been produced in the past three years (Nunan & Di Domenico, 2013). Finally, conversations about the ethical and interpretive dimension of big data analysis were not as sophisticated in 2001 as they are today (Boyd & Crawford, 2012; Data & Society Research Institute, 2014; Lennon 2014).

Increasingly generated from a rapidly expanding set of media technologies, big data now can be said to include five key categories: public data, private data, data exhaust, community data, and data generated through self-quantification (George, Haas, M. R., & Pentland, 2014). Public data are defined as those typically maintained and made available by a democratic government as a common good, whereas private data are held as a proprietary asset by corporations and private organizations. Data exhaust refers to passively collected, so-called "non-core" data that seemingly holds little interest on its own, but which can be recombined with other data sources to create new value. Examples include purchase transactions and Internet searches, which become valuable to advertisers, sociologists, and law enforcement when combined with other axes of information, such as demographic, identity-based, and geospatial data. Community data incorporate generally-unstructured or heterogeneous, volunteered data, primarily textual in nature, into informal, crowd-sourced networks that can be used to capture trends, such as consumer reviews or Twitter feeds. Finally, data of self-quantification are (mostly) deliberate recordings by individuals of their own personal actions and behaviors, tracked through devices such as health-monitoring wristbands and generally uploaded to proprietary cloud-computing databases by mobile applications (George et al., 2014). In 2001, most of these types of data were not available for analysis using current powerful computational techniques able to reveal trends within and among gigantic socioeconomic and cultural data sets (George et al., 2014). While contemporary text- and data-mining methods can help investigators draw a sharp outline of one individual's actions from his or her interactions at a group level (Nunan & Di Domenico, 2013), and can assist investigators in understanding changes in the behavior of a single individual and in the emotional tone or "sentiment" of his writings (Liu 2010), access of investigators to born-digital information meeting the commonly-accepted definition of "big data" (data both large in volume and high in variety and velocity) was much more limited at the time of the attacks.

Relevant Evidence

A significant amount of circumstantial and scientific evidence implicating Dr. Ivins led the U.S. DOJ to determine that he had been solely responsible for mailing the anthrax letters in September and October of 2001. The DOJ further found that Ivins had the opportunity and ability to produce and mail the spores.

Following this identification, Chief Judge Royce C. Lamberth of the U.S. District Court for the District of Columbia authorized a report from the Expert Behavioral Analysis Panel (EBAP) cited above. The panel was charged with examining "the mental health issues of Dr. Bruce Ivins and what lessons can be learned from that analysis that may be useful in preventing future bioterrorism attacks."(Saathoff *et al*, 2010). Notably, the EBAP was not specifically authorized by Judge Lamberth to use algorithmic techniques to seek patterns or behavioral anomalies, or to conduct sentiment analysis of Ivins' electronic communications, which represented only a small fraction of the available information on the case. Voluminous non-digitized records included interviews, application forms, security assessments and health data. The resulting EBAP Report was therefore based upon a review of Dr. Ivins' sealed psychiatric records and of the FBI and U.S. Postal Service's extensive investigative file—not on a computer-assisted "distant reading" of the case. Relying upon the expertise of the Panel's nine members, the EBAP Report held that the investigative file and sealed psychiatric records supported the Department of Justice's determination that Ivins was responsible for the crimes, in that Ivins "was psychologically disposed to undertake the mailings; his behavioral history demonstrated his potential for carrying them out; and he had the motivation and the means." The Report further held that Ivins' psychiatric records "offer considerable additional circumstantial evidence in support of the DOJ's finding" (Saathoff *et al.,*2010).

Through its investigation, the panel found that Dr. Ivins had led a secretive, compartmentalized life with criminal behaviors dating back to his time in college four decades earlier. A meticulous scientist, Ivins was careful about divulging incriminating evidence, revealing his criminal behaviors mainly to select mental health professionals who were bound by confidentiality rules preventing them from providing information to authorities. It was not until after Ivins' death on July 29, 2008 that the court order issued by Chief Judge Lamberth allowed access to all of his available mental health records. In addition, also following his death, FBI agents removed "two public-access computers from the Frederick County Public Libraries' C. Burr Artz Library in downtown Frederick, Maryland" (American Libraries Magazine, 2008). Information gleaned from digital forensic analysis of these machines was also made available to investigators.

Although the sophisticated toolsets and fund of knowledge possessed by bioinformatics researchers today did not exist at the time of the anthrax attacks, the first focus of investigation had to be on the spores themselves. Bacterial pathogenomics was in its infancy at the time of the mailings, which were in fact a major impetus to the growth and development of the field (Pallen and Wren, 2007). Although the scientific basis of the analysis of BSATs is beyond the scope of this paper, it is worth noting that analysis of the mailed anthrax spores quickly proved them to be of the AMES strain. This was a highly lethal and identifiable form of anthrax then being used to develop an anthrax vaccine required on a large scale by the United States military. What took much more time and effort, requiring the work of numerous independent laboratories and scientists, was the painstaking phylogenetic tracing of mutations, now known as "microbial forensics." These specific signatures were ultimately found in only one original source—the strain maintained by Dr. Bruce Ivins at USAMRIID in Fort Dietrich, Maryland (DOJ 2010).[3]

The double-blind scientific process of experimentation yielded a great amount of information over time, but it is important to understand that it was not available to law enforcement during and immediately after the attacks—only in the years that followed. Further, Dr. Ivins' decision to insert himself into the investigation from an early stage, and without the authorization of superiors, served to impede the more traditional and circumstantial investigation. According to the final report issued by the Department of Justice, federal investigators learned in interviews that Ivins was "driven by obsessions" and that he had a longstanding practice of using false identities, "especially when mailing packages from distant post offices." When confronted with damning evidence, Ivins was not able to provide reasonable or consistent explanations for his behavior, and "took a

[3] Ongoing scientific inquiry and examination of the case has continued, most notably with a 2011 National Research Council review, undertaken at the FBI's request. The NRC's finding is akin to the thesis we put forward here: that it is not possible to reach a definitive conclusion in this case on the basis of one type of evidence or method of analysis alone.

number of steps to stay ahead of the investigation." But because a large number of independent scientists performed experiments yielding objective data that allowed investigators to trace the anthrax to Ivins' flask, he was not able so easily to obstruct the scientific process. The vector for the murder weapon, a flask identified as RMR-1029, was found to be in Ivins' sole possession.

In the course of their work, investigating scientists learned that Dr. Ivins possessed significant expertise in the type of equipment that had been used to prepare the spores for insertion into the mailed envelopes. His technical prowess in creating highly purified anthrax spores was unquestioned, given his significant role in leading the vaccine program.

The investigation then turned toward psychological predisposition, behavior and motive, the area of the EBAP's expertise. An examination of Ivins' email correspondence with supervisors regarding the future of his anthrax program revealed that the program was in jeopardy, in part due to questions from Senator Daschle and other lawmakers regarding the safety of the anthrax vaccine that he had developed. According to the Department of Justice's conclusion, Dr. Ivins' life's work appeared destined for failure, absent an unexpected event (2010).

Examination of records dating back to his time as an undergraduate revealed Dr. Ivins' long history of vengeful behaviors directed toward others. The son of a Princeton graduate, he aspired to attend Princeton while in high school, but ultimately matriculated at the University of Cincinnati. From childhood, his family life was marked by significant emotional abuse as well as the repeated physical violence that his mother directed toward his father.

Preoccupied with fantasies of revenge, Ivins threatened college roommates with biological agents and shot pistols in occupied University buildings. He felt easily slighted. While an undergraduate, his romantic overtures toward a member of the Kappa Kappa Gamma sorority chapter at the University of Cincinnati were rebuffed. He then spent the rest of his life preoccupied with vengeance toward the national sorority and certain sorority members of his acquaintance. In the final year of his life, Ivins admitted that he had burglarized and vandalized a sorority house and made plans to kill Kappa Kappa Gamma members. Through thorough investigation, it was determined that both sets of anthrax letters sent to the media in September and to the Senate in October 2001 were mailed from the same postal collection box in Princeton, New Jersey. Significantly, this mailbox was located across the street from the Princeton campus and next to the site of Princeton's Kappa Kappa Gamma administrative offices.

This kind of deep insight into Ivins' psychological state—specifically the likely association in his mind among Princeton University, Kappa Kappa Gamma, and the desire for revenge and validation—came only from a close reading of mental health records and relevant evidence held in small, sparse, and heterogeneous datasets. Insights like these are difficult to glean from data analysis at scale, which typically requires large, dense, and relatively uniform (or uniformly-encoded) sets of information. However, taken together with data gathered by the U.S. Postal Inspection Service and the Federal Bureau of Investigation, including information generated or discovered by biogenomic investigators, digital forensic analysts, and creators of psychological and other health records, some elements of the case—if examined today—might lend themselves to sentiment analysis, authorship attribution, and forms of so-called "distant reading" or pattern analysis at scale (Moretti, 2005), (Moretti, 2013).

Potential for Stylometric and Sentiment Analysis

Bing Liu defines sentiment analysis simply, as "the computational study of opinions, sentiments and emotions expressed in text" (2010). Sentiments mined from text corpora of any size may express attitudes or judgments, reveal affect or a psychological state, or contribute to the emotional and aesthetic effect an author wishes his or her words to have upon an audience. Classification of utterances in sentiment analysis can occur either through supervised or unsupervised machine learning but, like all natural language processing tasks, these techniques pose no simple solutions and rest on "no easy problems" (Liu 2010). Similarly, stylometry—most often associated with authorship attribution, which uses similarities in vocabulary and phrasing to suggest the originator of a disputed text—applies a constellation of computational linguistic techniques to complex problems in human language. Examples include the notable early case of the contested authorship of the Federalist Papers (Mosteller and Wallace, 1964) and the more recent attribution of a pseudonymous crime novel to *Harry Potter* author J.K. Rowling (Juola, 2014). Computational analyses of style have also been used to suggest the gender or personality attributes of a writer, but here—as with authorship determination—the standards of proof and of admissibility of evidence in forensic application are necessarily much higher than in literary or historical study (Juola, 2006). This is further complicated by the typically shorter and more fragmentary nature of texts relevant to forensic examination—a difficult problem, but not one that has proven insurmountable (Chaski, 2005).

The DOJ Final Report makes data-driven determinations: "Dr. Ivins made many statements, and took many actions, evidencing his guilty conscience." Many of these statements were made verbally and in interviews given to federal law enforcement. However, the bulk of the textual evidence in the case, often inconsistent and contradictory, was found in emails from Ivins' workplace, which contained words and phrases indicative of his emotional state. Because Ivins was a civilian scientist who began his job at USAMRIID in Fort Dietrich in December of 1980, he communicated through email from the time it became available to his laboratory. As such, the extent of his email correspondence is significant, especially because he addressed colleagues via email with both professional and personal concerns, and because it opens the possibility of a longitudinal study—of comparison over time. Although Ivins attempted to extensively delete potentially incriminating emails dating from the period leading up to the anthrax mailings, he was unsuccessful.[4] As federal agents focused upon his laboratory, he remained unaware that his emails had been automatically saved within his computer system and were therefore available for review.

[4] Dr. Ivins also had also a huge corpus of hand written letters to aid in comparisons. He used both electronic and hand written documents that helped facilitate effective compartmentalization, thus decreasing the potential for investigators to access all of his writings for analysis.

Following the First Gulf War and the claims by some that Ivins' anthrax vaccine may have been responsible for "Gulf War syndrome," a constellation of symptoms arising in military personnel who were given the vaccine, Dr. Ivins was subjected to increasing public criticism for his work. He was also required to respond to Freedom of Information Act requests. Additional themes gleaned from a reading of his emails in this period include a sense of abandonment in his personal life. The Department of Justice Final Report notes that "Ivins's e-mail messages revealed a man increasingly struggling with mental health problems." In addition to voicing frustration, Dr. Ivins expressed anger in his correspondence. As the investigation proceeded, Dr. Ivins shifted blame to others, both in interviews with law enforcement as well as in emails. In particular, he shifted blame to close colleagues who worked with him in the laboratory, including a former colleague whom, at one point, he planned to poison.

The voluminous emails Ivins sent from his government account are revealing in that they address his ongoing substance abuse as well as his feelings of frustration, anger, and rage. Any examination of these office emails as a digital data corpus would be incomplete, however. Dr. Ivins also used numerous pseudonyms in communicating on various websites, including the Wikipedia site for the Kappa Kappa Gamma sorority and in blog posts that revealed his homicidal plans toward an actress in a reality television series. Also, according to the DOJ findings, Dr. Ivins had long been fascinated with codes and secrecy. He referred repeatedly to a favorite book describing the steganographic use of DNA codons—three-letter sequences—that could be embedded within a seemingly normal communication in order to transmit secret messages. It is therefore possible that further textual evidence in this case has remained undiscovered—perhaps even hidden in plain sight. It is also possible that various sentiment analysis techniques could be applied retrospectively to the Ivins corpus, as a concrete experiment in determining their utility in cases like this. Do changes in tone correlate with evidence of criminal behavior? If so, does this imply that investigators—if properly authorized—might usefully scan for notable changes in sentiment across all the email correspondence coming from a lab under investigation? *Should* they? What precedent would this set? What impact would the inevitable chilling effect of this monitoring have on scientific communication, on a local and much larger scale?

Authorship attribution algorithms were likewise not applied to the problem of analyzing Ivins' writing style against that of the anthrax letters (and indeed, even if such approaches had been commonplace among investigators, it is not clear that a sufficient writing sample would have been possible to attain, given the brevity of the letters) (Chaski, 2005). Nonetheless, Dr. Ivins's use of written language in electronic messages was deemed by expert human readers to be similar to the language used in the anthrax mailings.[5] Similarly, this corpus of writing—taken alongside other real-world examples—could provide fodder for experiments in authorship attribution by law enforcement.

Potential for Further Pattern Analysis and Visualization

Beyond the insights that might be gained through sentiment and stylometric analysis of written language, the Amerithrax case illustrates potential for pattern analysis and visualization of mid-sized data sets. These data include biogenomic corpora as well as collected transactional information, such as pharmaceutical prescription information, diagnostic codings, and postal manufacturing and financial data. Perhaps even more significant in this case are records of Dr. Ivins' behavior: specifically, of his comings and goings. Ivins' access to restricted anthrax spores was recorded with the help of a digitized entry log. This log detailed his vastly increased laboratory hours during the nights and weekends just prior to each mailing.

Although data relating to scientists' hours spent in the "hot suite" was available within the research facility's security system, it was not accessed until biogenomic evidence led investigators to USAMRIID and Ivins' laboratory. While it may seem obvious now that this type of passively-collected data would be of interest, Ivins had made statements that focused suspicion on other quarters and was therefore able to divert the investigation.

[5] To the extent that it was possible at the time, the Federal Bureau of Investigation (FBI) did attempt to analyze the brief anthrax threat letters against its existing database of written threats. No prior authored threats of Dr. Ivins existed in the database. Therefore, automated canvassing did not yield a match similar in content or style.

Important in this case were changed patterns not only in the number of hours he spent in the highly restricted anthrax laboratory, but also in the timing of Ivins' presence there. A dramatic and atypical increase in hours during August, September and early October, prior to the postmarking of the second group of letters, occurred at times when he was alone in that laboratory – on weekends and at night. When questioned about this, Ivins was evasive and vague in his answers. He could point to no scientific endeavor that would have explained his long and unusually-timed hours, other than to say that they occurred during a period of stress at home which prompted him to prefer the laboratory to the presence of his wife and children.

In the days, weeks, and months following the attacks, Dr. Ivins behaved in ways that seemed quite helpful to investigators within the FBI and US Postal Inspection Service. In addition to privately identifying no less than seven colleagues as possible anthrax mailers in order to divert attention from himself, he also engaged in behaviors that may have been designed to elicit positive attention, positioning himself as a researcher possessed of expertise that could benefit his colleagues during the investigation, or which could provide a public service.

Notably, these positive behaviors (not of a type subject to self-quantification or passive collection of "data exhaust") occurred just *after* the first group of letters had been postmarked, but *before* medical symptoms suggesting anthrax infection in any recipients could occur. Shortly following the postmarking of the initial mailings, Ivins re-introduced himself to a former colleague in the form of an email. In it, he indicated that, in the wake of the 9-11 attacks, he was prepared to assist the country in the event of bioterrorism. In the absence of any specific warning or sign of biological attack, this struck the former colleague as odd. Also within the narrow window between the postmarking of the first letter and publicized symptoms in recipients, Ivins joined his local chapter of the American Red Cross. His application specified that his occupation involved anthrax research. (In reviewing numerous other forms and applications that Ivins had filled out over the decades, the EBAP found it significant that this appeared to be the only moment at which he identified himself as someone versed in anthrax research.) Following the deaths of his victims, Ivins inserted himself into the official investigation by appearing at a pond that was being searched for anthrax spores. Although advised by colleagues that it would be inappropriate to participate in the investigation in his role as a Red Cross volunteer, he ignored that advice and was present during the search until recognized by an investigator and escorted from the area. Nonetheless, Ivins' provision of scientific expertise in apparent response to the anthrax mailings earned admiration from colleagues and supervisors. In fact, in a public ceremony in 2003, he was awarded the highest US Army Civilian Award, presented personally by the Secretary of the Army.

Absence of evidence, is not necessarily evidence of absence. It is important to note that Ivins sometimes evaded opportunities to track his behaviors. For instance, although he had a self-admitted, decades-long history of making midnight drives to other states in order to burglarize sorority houses, Ivins' wife and family were left seemingly unaware of his late night and long-distance travels. He left no credit card records for gasoline or other purchases, and he may have in fact taken further steps to avoid surveillance or obstruct justice. Still, significant behavioral and transactional evidence was amassed as part of the investigation, and that evidence, mapped along temporal and geographic axes with the help of contemporary visualization tools and techniques, would likely reveal patterns unnoticed by investigators at the time of the case and therefore unavailable to behavioral analysts. Even simple visualizations in the form of timelines, maps, scatter plots, and charts can serve to focus investigators' attention. If dense, complex information related to Ivins' activities could have been compared visually against the recorded actions of other scientists under investigation in his lab—or even against his own behavior in less pressured periods—anomalies suggesting fruitful lines of inquiry might have sooner emerged.

However, just as we find in stylometric and sentiment analysis that the very "complexity of language implies that automated content analysis methods will never replace careful and close reading of texts" (Grimmer and Stewart, 2013), data visualization, too, must be understood as a complex, humanistic act depending on and demanding interpretation.

Like the human beings whose behaviors they attempt to represent, algorithmic data visualizations can over-emphasize and obscure information—both inadvertently and by design. The well-known work of statistician and political scientist Edward Tufte on visualization and information design is foundational here (Tufte, 1997; Tufte, 2001), as is Johanna Drucker's warning that technologies of display borrowed from the natural and social sciences can render those who study humanistic datasets "ready and eager to suspend critical judgment in a rush to visualization." Drucker holds that all human-generated data must instead be understood as *capta*—not as something rationally observed, neutrally presented, and given, but rather as that which is *taken*, in the form of subjective representations demonstrating and demanding the "situated, partial, and constitutive character of knowledge production, the recognition that knowledge is constructed" by people with inherent, inescapable agendas or biases, blind-spots, and points of view (Drucker, 2011).

Final Words: Interpretation and Insider Threat

Why are the concerns we highlight here particularly relevant to insider threat cases in a "big data" age? What qualities of these investigations demonstrate how algorithmic data analysis is simultaneously promising—indeed necessary, as crimes are committed in an increasingly networked, digital world—and yet clearly in need of further critical examination? We have used the 2001 Amerithrax case to demonstrate how insider threat investigations pose examples of individuals behaving in traceably anomalous ways, often within groups whose sensitive missions open them to a particularly high level of monitoring and data collection. Cases like these demand that investigators visualize and identify patterns emerging from dense, rich, and very large sets of behavioral and transactional data that play out across metadata-bearing axes like space and time. They also provide opportunities for computational techniques possible within smaller sample sets—such as sentiment analysis and forensic authorship attribution—to be tested and refined now that mass-digitized textual corpora are available for comparison, experimentation, and advancement of machine learning and natural language processing.

Most interesting to us, however, as behavioral analysts and law enforcement agencies continue to add algorithmic approaches to their investigatory toolsets, are not questions about what is possible, but about what is advisable. The Ivins case—ending as it did in the suicide of a suspect under investigation and subsequent, costly and time-consuming rounds of scientific and psychological review—proves useful in foregrounding the concerns that insider threat investigations raise with regard to data collection, ethics, interpretation, and use. Just as life scientists are examining their ethical obligations vis-à-vis dual use research in an age of bioterrorism (Kuhlau et al, 2008; Somerville & Atlas, 2005), forensic investigators should operate within and advocate for rigorous legal and ethical constraints. To date, debates about psychological ethics and national security have focused largely on the involvement of mental health professionals in prisoner interrogation (Ackerman, 2014; APA, 2013). A concomitant conversation should be opened about the ethics of big data use in forensic psychiatry and criminal profiling.

Critical here will be an effort to broaden the understanding that algorithmic data analysis and visualization are no substitute for close reading and interpretation by trained and intuitive psychiatric professionals. These techniques are rather an aid to elucidation, serving to focus investigators' attention and provide further forms of evidence that *must be interpreted* as to behavior and psychological state. Here, we can usefully bring to bear lessons learned from the application of computing to interpretive problems in humanities scholarship. These range from the impact of implicit assumptions and biases on research questions and the assembly of datasets (Sculley & Pasanek, 2008) to the reminder that subjective and objective concerns must be kept in useful tension in text analysis, data mining, and visualization (Clement, 2013). A comprehensive review by the Council on Library and Information Resources, of eight large-scale digital humanities projects funded under an international "Digging into Data Challenge" scheme in 2009 and 2011, found that "humanistic inquiry," like human behavior, is "freeform, fluid, and exploratory; not easily translatable into a computationally reproducible set of actions." This review identified a characteristic need that data-driven projects in the humanities share with the application of data analytics to investigations of insider threat: the need to address inevitable gaps "between automated computational analysis and interpretive reasoning" that can "make allowances for doubt, uncertainty, and/or multiple possibilities" (Williford & Henry, 2012).

Forensic behavioral scientists, like other investigators of crimes, must recognize the potential of data science to resolve insider threat cases more quickly and effectively, adding crucial evidence to the positive identification of perpetrators and perhaps saving lives. But they should feel an equally great responsibility to employ new technologies wisely—in accordance with the law and their professional ethics, and in ways that augment rather than supplant close reading and interpretive expertise.

Reference List

Ackerman, S. "CIA's Brutal and Ineffective Use of Torture Revealed in Landmark Report." *The Guardian.* Accessed August 9, 2014. http://www.theguardian.com/us-news/2014/dec/09/cia-torture-report-released

American Libraries Magazine. "FBI Seizes Library Computers; Anthrax-Case Link Suspected."6 August 2008. Accessed August 9, 2014. http://www.americanlibrariesmagazine.org/archive/2008/august2008/anthraxcomputersseized

American Psychological Association (APA). 2013. "Policy Related to Psychologists' Work in National Security Settings and Reaffirmation of the APA Position Against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment."*Council Policy Manual.* Accessed 6 September 2014. http://www.apa.org/about/policy/national-security.aspx

Boyd, d. & Crawford, K. 2012. "Critical Questions for Big Data." *Information, Communication & Society.* 15:5. 662-679.

Chaski, C. E. 2005. "Who's at the keyboard: Authorship attribution in digital evidence investigations." *International Journal of Digital Evidence.* 4:1.

Chessick, R.D. 1990. "Hermeneutics for Psychotherapists." *American Journal of Psychotherapy.* 44:2.256-73.

Clement, C. 2013. “Text Analysis, Data Mining, and Visualizations in Literary Scholarship.”*Literary Studies in the Digital Age: An Evolving Anthology*. Modern Language Association. (editors Price, K. and Siemens, S.) Accessed 6 September 2014. http://dlsanthology.commons.mla.org/text-analysis-data-mining-and-visualizations-in-literary-scholarship/

Data & Society Research Institute. 2014. *Event Summary: The Social, Cultural, & Ethical Dimensions of "Big Data" March 17, 2014 - New York, NY.* Accessed 6 September 2014. http://www.datasociety.net/pubs/2014-0317/BigDataConferenceSummary.pdf

Drucker, J. 2011. “Humanities Approaches to Graphical Display.” *Digital Humanities Quarterly* 5:11. Accessed 5 September 2014. http://digitalhumanities.org:8080/dhq/vol/5/1/000091/000091.html

George G, Haas MR, Pentland A, 2014, “Big Data and Management.” *Academy of Management Journal*, Vol:57, ISSN:0001-4273:321-326
Gold, M.K. (ed). 2012. *Debates in the Digital Humanities*. University of Minnesota Press: Minneapolis.

Grimmer, J. and Stewart, B. M. 2013. “Text as Data: the Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts.” *Political Analysis.* Oxford Journals: doi:10.1093/pan/mps028

Juola, P. 2006. “Authorship Attribution.”*Foundations and Trends in Information Retrieval* Vol. 1, No. 3 (233–334).doi: 10.1561/1500000005

Juola, P. 2014. “The Rowling Case: A Proposed Standard Analytic Protocol for Authorship Questions.” Paper presented at *Digital Humanities 2014*, Alliance of Digital Humanities Organizations. Extended abstract available: http://dh2014.org/Accessed 6 September 2014.

Kuhlau, F. et al. 2008. “Taking Due Care: Moral Obligations in Dual Use Research.” *Bioethics*. 22:9.477-487. doi:10.1111/j.1467-8519.2008.00695.x

Lennon, B. 2014. “The Digital Humanities and National Security.” *differences: A Journal of Feminist Cultural Study.* 25:1. 132-155.

Lichtblau, E. 2008. “Scientist Officially Exonerated in Anthrax Attacks.”*New York Times*. Accessed August 9, 2014. http://www.nytimes.com/2008/08/09/washington/09anthrax.html

Liu, B. 2010. "Sentiment Analysis and Subjectivity". *Handbook of Natural Language Processing*. Second Edition. (editors: N. Indurkhya and F. J. Damerau). Preprint available: http://www.cs.uic.edu/%7Eliub/FBS/NLP-handbook-sentiment-analysis.pdf

Moretti, F. 2005. *Graphs, Maps, Trees: Abstract Models for a Literary History*. Verso Books: London.

Moretti, F. 2013. *Distant Reading*. Verso Books: London.

Mosteller, F. and Wallace, D. 1964. *Inference and Disputed Authorship: The Federalist Papers.* Addison-Wesley: Reading, MA.

National Research Council. *Review of the Scientific Approaches Used During the FBI's Investigation of the 2001 Anthrax Letters*. Washington, DC: The National Academies Press, 2011.

Nowviskie, B. 2014."Algorithm." *The Johns Hopkins Guide to Digital Media*. The Johns Hopkins University Press: Baltimore. (editors L. Emerson, B. Robertson, and M-L. Ryan)

Nowviskie, B. 2014a. "Ludic Algorithms." *PastPlay: Teaching and Learning History with Technology*. University of Michigan Press: Ann Arbor. (editor: Kevin Kee)

Nunan, D., & Di Domenico, M. 2013. "Market research and the ethics of big data."*International Journal of Market Research*. 55(4), 2-13.

Pallen, M. J., & Wren, B. W. 2007. "Bacterial pathogenomics." *Nature*. Volume 449. 18 October 2007. doi:10.1038/nature06248. 835-842.

Pasternack, A. 2014. "In Our Google Searches, Researchers See a Post-Snowden Chilling Effect," *Motherboard*. Accessed 1 September 2014. http://motherboard.vice.com/read/nsa-chilling-effect

Saathoff, G. and DeFrancisco, J. 2010.*The Amerithrax Case: Report of the Expert Behavioral Analysis Panel*, Research Strategies Network, August 2010.

Sculley, D. and Pasanek, B. 2008. "Meaning and mining: the impact of implicit assumptions in data mining for the humanities." *Literary and Linguistic Computing*.23:4. 409-424.

Shaw, E.,Fischer, L. and Rose, A. 2009. *US Department of Defense Personnel Security Research Center Technical Report 09-02.* Accessed on 1 September 2014. http://www.dhra.mil/perserec/reports/tr09-02.pdf

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., Flynn, L. 2012. *Common Sense Guide to Mitigating Insider Threats*, 4th Edition (Technical Report CMU/SEI-2012-TR-012). Pittsburgh: Software Engineering Institute, Carnegie Mellon University. Accessed on 1 September 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017

Somerville, M. and Atlas, R. 2005. "Ethics: A Weapon to Counter Bioterrorism." *Science*. 25 March 2005. Vol 307. Issue 5717. 1881-1882.

Transcript of Powell's U.N. Presentation, Part 5. Biological Weapons Program. CNN, 2003. Accessed on 24 August, 2014. http://edition.cnn.com/2003/US/02/05/sprj.irq.powell.transcript.05/

Tufte, E. 1997. *Visual Explanations: Images and Quantities, Evidence and Narrative.* Graphics Press: Cheshire, CT.

Tufte, E. 2001. *The Visual Display of Quantitative Information*. Second Edition. Graphics Press: Cheshire, CT.

United States Department of Justice (DOJ). 2010.*Amerithrax Investigative Summary*. February 19, 2010. Accessed on 9 August 2014. http://www.justice.gov/archive/amerithrax/docs/amx-investigative-summary.pdf

United States Federal Bureau of Investigation (FBI), 2011. "FBI and Justice Department Response to NAS Review of Scientific Approaches Used During the Investigation of the 2001 Anthrax Letters." 15 February 2011. Accessed 6 September 2014. http://www.fbi.gov/news/pressrel/press-releases/fbi-and-justice-department-response-to-nas-review-of-scientific-approaches-used-during-the-investigation-of-the-2001-anthrax-letters

Weisman, S. 2005. "Powell Calls His U.N. Speech a Lasting Blot on His Record. *New York Times*. 9 September 2005.Accessed August 24, 2014. http://www.nytimes.com/2005/09/09/politics/09powell.html

Williford, C. and Henry, C. 2012. *One Culture: Computationally Intensive Research in the Humanities and Social Sciences: A Report on the Experiences of First Respondents to the Digging into Data Challenge.* Council on Library and Information Resources. CLIR pub151. Accessed 6 September 2014. http://www.clir.org/pubs/reports/pub151