

GOOGLE'S APPROACH TO PREVENTING VIOLENT CRIME ON CAMPUS:
THE ROLE OF DATA MINING AS A THREAT ASSESSMENT TOOL

by

Michael D. Morris
CSU Channel Islands Police Department

September, 2011

COMMAND COLLEGE CLASS 49

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it – creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

GOOGLE'S APPROACH TO PREVENTING VIOLENT CRIME ON CAMPUS: THE ROLE OF DATA MINING AS A THREAT ASSESSMENT TOOL

Introduction

He hadn't taken his medication in weeks – didn't need it. His clarity and focus over the past couple of months was unlike it had ever been before. His sweating hands firmly clutched the plastic grips of the twin Glock .40 caliber pistols he had ordered online as he stood in the hallway preparing to enter the campus library through a side door.

If only there would have been a way to look into a magic crystal ball and see that this horrific confrontation was about to occur, it could have been prevented. In the aftermath of nearly every large-scale act of campus violence in the United States, subsequent investigation has revealed that early warning signs had been present, but not recognized or acted upon. As a response, nearly all college and university campuses have developed threat assessment teams, whereby key members of various campus groups come together on a regular basis to share information and discuss troubling student behavior. Sharing and analyzing this information provides the university an opportunity to determine the level of threat that might exist and to take appropriate steps to intervene in a student's life in an effort to prevent more significant behavior. Unfortunately, in their efforts to prevent a violent crime from occurring, these teams are only able to assess students whose issues have already manifested in problematic behaviors that have been noticed by members of the campus community and brought to the attention of team members.

This effort to prevent violent crime still remains somewhat reactive in its approach. Existing technology offers campuses an opportunity to possess their own crystal ball. In an effort to prevent large-scale acts of violence at colleges and universities, campuses must be prepared to utilize technology to its fullest extent to identify the potential for violence before it

happens, so officials can take steps to intervene. The necessary next step is to use data mining to identify and mitigate the potential for tragedy on our campuses.

Violence on Campus

Brutal massacres such as those that took place at Virginia Tech and Northern Illinois Universities create significant and lasting damage to a university community. Even the quickest and most effective police response to a major act of violence won't be good enough. Lives will be lost and the university's name will be forever branded in the history books.

With increasing frequency, the 42 shooting rampages on college and university campuses in the United States between January 1, 1990 and May 31, 2009 resulted in 94 people killed (excluding shooter deaths) and 92 wounded (Kaminski, et.al, 2010).

To more effectively prevent these mass murders, carried out by lone gunmen or coordinated assembly of killers on campuses, threat assessment teams need access to a greater wealth of information beyond reports of students having acted out. They need access to information about a student's psychological state of mind, which can often be difficult to see. They also need information that might indicate a student is in the process of developing a strategic attack, which can also be very difficult to discern through traditional means.

Aggressors in the University Environment

According to John Byrnes, the President of the Center for Aggression Management, there are two types of aggressors – primal aggressors and cognitive aggressors. A primal aggressor reacts in the heat of passion to some type of stimulus, such as coming home to find his spouse in bed with another person, and explodes, exhibiting behavior that is fueled by rage, anger, and humiliation (Byrnes, 2002). Although this is the type of behavior that typically comes to the attention of threat assessment teams, it is rarely the type of behavior exhibited by school shooters

(Sokolow & Lewis, 2009). Research has shown that school shooters are typically cognitive aggressors who systematically plan their attacks and carry them out methodically and tactically, often intending to conclude with their suicide (Byrnes, 2002). Considering the prevalent use of the Internet for research and communication, one would logically conclude these aggressors might leave evidence of their intent in electronic databases as they plan and prepare for the assault.

Most college and university campuses in California provide each of their students with an email address, personal access into the university's network, free use of campus computers, and free wired and wireless Internet access for their web-connected devices. Students use these campus resources for conducting research, communicating with others, and for other personal activities on the Internet including social networking. University officials could potentially utilize data mining techniques to isolate and analyze this data, since it is already under their control. The analysis could then be screened to predict behavior to identify when a student's online activities tend to indicate a threat to the campus community.

If university officials were to learn an individual student had conducted extensive online research about the personal life and daily activities of a particular faculty member, posted angry and threatening comments on his Facebook wall about that professor, shopped online for high-powered firearms and ammunition, and saved a draft version of a suicide note on his personal network drive, would those officials be interested to have a conversation with that student, even though he hadn't engaged in any significant outward behavior? Certainly. This information, which now may reside in the university's IT system, would allow the campus to strategize a swift and effective intervention, and take proactive steps to prevent violent behavior from ever

occurring. Interestingly, the technology already exists to allow university officials to use data mining techniques to predict future criminal behavior.

The Gift of Data Mining

Our online activities are under constant surveillance by companies eager to learn about our individual interests. Their findings are used for marketing purposes to target consumers with goods and services based on our specific interests. How does Amazon.com know what types of books I'm interested in reading? How did my Gmail account find out I'm an Oakland Raiders fan? These examples are instances of data mining.

The Internet has become a staple in daily life of the 21st Century. From searching the web, to shopping, to social networking, and beyond, it has become completely necessary to utilize the Internet's resources to keep up with the demands of society. As information stored in various hard drives and server farms has expanded exponentially, so too have the methods to analyze it. Predictive analytics, or data mining, has been used across a broad spectrum of sectors and business to help identify potential customers, discern patterns, and refine demographic information for voting, purchasing, and other uses. The utility that comes with the capacity to predict the future is limitless.

Data mining involves a process of applying specifically designed algorithms to a body of electronic data to identify patterns and transform the data into usable information. Data mining is a form of behavioral surveillance, and it can be used to predict, with amazing accuracy, the propensity for a person's future behavior. For instance, credit card companies are using data mining techniques to predict when a married couple is preparing to divorce. This is being done as a risk management tool by lending institutions, since people who are going through a divorce are more likely to miss payments on their credit cards (Ciarelli, 2010).

The covert use of data mining to predict future behaviors is increasing. Websites such as Yahoo and Google routinely use data mining for behavioral targeting to customize the types of advertisements that are sent to particular users. A person's online activities are recorded by electronic markers left on the web browser, and companies use that information to direct advertisements specific to the person's interests (Hof, 2009). Organizations such as Rapleaf, a San Francisco-based data mining firm, use social media monitoring techniques to draw conclusions about people based on the behaviors of their friends on sites like Facebook and MySpace. They claim that "information about your friends' behavior can be used to better predict your behavior". In doing so, creditors, for example, may choose to approve or deny a person's credit application based, in part, on payment histories of his Facebook friends (Conley, 2009).

Federal Fusion Centers also collect and share information from numerous public databases with a focus on determining crime trends and predicting crimes before they occur (EPIC, n.d.). Organizations like the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) serve as watchdogs over government intrusions. They have repeatedly forwarded legislation to limit the government's access to personal information (Hylton, 2009; EPIC, n.d.). Privacy groups assert these Centers have gone too far, and have used this information for purposes beyond the prevention of terrorism. Still, Fusion Centers continue to operate effectively across the country, at both the federal and local levels, using data mining techniques to keep tabs on criminals.

Computer engineers design data mining algorithms to search for specific patterns that, when analyzed collectively, tend to indicate the likelihood of a particular outcome. Have you ever had a credit card transaction declined because the bank had noticed an unusual pattern of

spending on your account? Through data mining, the bank had drawn the conclusion your credit card had been stolen. It would logically follow that mining algorithms could be easily designed to predict the potential for planned or considered campus violence as well.

The business community makes good use of data mining tools for marketing analysis, as do law enforcement agencies in their search for terrorists. Society has become accustomed to invasions of their online privacy, and the trends indicate the personal privacy of individuals is becoming less and less important each day. Taking a logical step forward, it is reasonable to consider the use of data mining to bring otherwise concealed information on the activities of cognitive aggressors to the attention of the authorities for the purpose of preventing violent crimes. The challenge with doing so involves concerns over privacy issues, as well as due process considerations.

Issues of Privacy and Due Process

Although privacy emerges as the primary concern over this type of behavioral surveillance, society has been systematically forfeiting its own rights to online privacy over the past several years through the continued and increased use of services on the Internet. Social networking sites and search engines store and divulge personal information accessible to the world each day, yet individuals continue to utilize them in increasing numbers.

The issue of data mining recently made headlines when the United States Supreme Court struck down a 2007 Vermont law restricting pharmaceutical companies from using data mining to enhance marketing efforts as being unconstitutional. The Court ruled the Vermont law violated the First Amendment by restricting the marketing work of the pharmaceutical companies, and the right to free speech outweighed the State's efforts to protect medical privacy (Biskupic, 2011).

Even in the face of an epidemic of identity theft and online predators, Internet users seem to demonstrate a laissez-faire attitude about protecting their personal information. Mark Zuckerberg, the Founder of Facebook, recently asserted that the increased sharing of personal information online has become the new “social norm”, and that users no longer have a basic expectation of privacy. A vast number of people have become comfortable posting detailed personal information on the Internet related to their interests and activities. In Zuckerberg’s opinion, online privacy is not something that Internet users expect. This view of the “social norm” prompted the Facebook CEO to modify Facebook’s default privacy settings, revealing significantly more personal information on account holders to the entire internet (Duncan, 2010).

The courts are ruling in various cases across the country that online activities are not necessarily protected by privacy rights. Two sheriff’s deputies in Georgia were fired after anonymously posting comments on Topix.com. The sheriff’s department had learned the true identities of the deputies using their IP addresses. The courts have ruled in many of these cases that companies like Topix.com must turn over the IP addresses of individuals when presented with a court subpoena (Cook, 2011). In one New York case, the plaintiff in a personal injury lawsuit was ordered to provide the user name and password for her Facebook and MySpace accounts to the defendant because there was evidence those sites contained photos which proved her injury case was false (Kaufer, 2010). Peter Canfield, a media attorney who represents The Atlanta Journal-Constitution newspaper, said, “People believe that they’re acting anonymously on the Internet, and to a certain extent that may be true. But people have virtually no privacy on the Internet. When you go online, you leave tracks that can be followed and traced.” (Cook, 2011). In spite of concerns about privacy, steps can be taken to ensure data mining does not adversely impact a student’s rights to due process.

Changing the Campus Culture

Resistance by campuses to engage in passive behavioral surveillance through data mining will leave threat assessment teams to continue operating as they currently do – analyzing outward behavioral problems that have been witnessed by others in the campus community and brought to the attention of the team. As long as no violent crimes happen to occur on campus, this approach will probably be fine. As with any crime prevention program, no one can ever truly know how many crimes have actually been prevented as a result of the program. From warnings, to counseling referrals, to suspension from the university, threat assessment teams have launched many interventions in an effort to disrupt patterns of problematic behavior exhibited by students. Still, there's no way to know – absent a subsequent confession – that the team's efforts prevented a crime from occurring. The fact remains that large-scale violent acts continue to occur on college and university campuses each year, despite the efforts of threat assessment teams. Enhancing the capacity of the threat assessment team through data mining is the next natural step in their development.

In collaboration with the campus' legal counsel, threat assessment teams will need to develop intervention protocols to guide the use of information yielded through data mining techniques. It will likely be inappropriate to take punitive action against a student based solely on a report produced by data mining algorithms, unless that report is accompanied by specific behaviors that can be articulated. The data mining process can bring the individual student to the attention of the threat assessment team, but team members must independently evaluate the data with other relevant information to determine the appropriate intervention to take, if any.

When data findings trigger an alert regarding the existence of a potential threat, that information would initially be directed to the I.T. Department, who would be responsible for

bringing it to the attention of the threat assessment team. The team would examine and analyze the specific online activities that triggered the alert, critically assess whether the information indicates a threat, and then determine if an intervention is appropriate. If so, the team would collectively establish the steps to be taken and would coordinate the response. For the purposes of intervention, an important distinction must be made between violations of the law and violations of campus policy. Certainly, the campus may take action in both arenas, but the approach for each will be quite different.

When a person's online activities demonstrate the person has committed a crime, the intervention will be handled by campus police or local law enforcement agency, who will conduct further investigation applying existing legal protocols for detention, search, arrest, etc. When their online activities indicate a potential to threat to the campus but no crimes have been committed, any intervention must be handled administratively as a violation of, say, the campus' Student Code of Conduct. Campus policy violations can be enforced very effectively, usually by the office of the Dean of Students in collaboration with campus police, Judicial Affairs, and Counseling Services. Interventions for policy violations focus on correcting behavior or, if necessary, removing the person from the campus. They are often easier to enforce because the standard of proof is much lower than for criminal violations. Any intervention at this point would be choreographed with a design to prevent a future violent incident. In consultation with legal counsel, universities should establish strong and consistent guidelines for intervention to ensure due process rights are not violated. This will be the most crucial element of the project and an area that cannot be ignored. The existence of a civil rights violation is never the search itself – it's what is ultimately done with the fruits of the search.

Changing the Administrative Culture

At first glance, universities might shy away from the thought of conducting covert surveillance of the members of their communities by means of data mining. College and university campuses are accustomed to enjoying academic freedom and the open expression of ideas, and constituents might not feel comfortable with the feeling of being watched. Resistance to this idea could result in members of the campus community choosing to leave the university to avoid this level of oversight. Other concerns with the use of data mining as a threat assessment tool might include the potential for “false positives”, meaning that the data findings serve as the basis for intervention with a student when no real threat actually existed, or that data findings might conflict with the university’s social values. While those arguments may be valid within the current paradigm of an individual campus, that paradigm would change suddenly if a shooting rampage were to occur on that campus.

Since predictive technologies do currently exist, how long will it be before society comes to expect it? What will be the depth of liability for a University when a violent killing rampage occurs and the campus hadn’t done everything that could have reasonably been done to prevent it? In its 2008 annual whitepaper, the National Center for Higher Education Risk Management discussed campus risk management practices which should be taken to limit liability. In that report, they stated “In the aftermath of the Virginia Tech shootings, several prominent panels were convened around the country to examine the issue of violence in schools and, in particular, on college campuses, and to determine avenues that administrators can take to possibly mitigate future shooting events”. Some of the recommendations included, “...an increased effort at sharing of information...to provide better detection, intervention, and response to school shootings, increased educational awareness...regarding mental illness in college-and school-age individuals, modification of existing state and federal laws to allow for easier reporting of

information associated with...mental illness, and expansion of training in the area of behavioral analysis, threat assessments, and emergency preparedness for colleges and universities.”

(Sokolow & Hughes, 2008). There is a significant need for campuses to take steps to mitigate risk and reduce liability, particularly in the area of campus violence. Before long, campuses that haven't taken advantage of technology's capabilities will be criticized for failing to adhere to best practices. The reality is that colleges and universities should immediately begin planning implementation strategies for this new approach to violence prevention in an effort to avoid being left behind.

Conclusion

Within the next decade, the use of data mining as a threat assessment tool on university campuses should be the norm. It has all the makings of a best practice, and nearly all institutions of higher education will likely utilize this technology on a day-to-day basis. In the meantime, a few specific recommendations will help campuses prepare and position themselves for this reality.

Because University campuses are prime targets for large-scale acts of violence, have their own full-service computer networks, and operate comprehensive threat assessment teams, the use of data mining technology for violence prevention should begin there. Analysis by a threat assessment team, coupled with appropriate intervention, is crucial to prevent a violent crime from occurring. Therefore, it is logical the team would have the ability to consider all relevant information, including that which only technology might be able to reveal.

It remains true that there is no way to determine how many crimes are actually prevented through the efforts of crime prevention. It is also true that no single crime prevention program can be 100 percent effective, 100 percent of the time. If we had access to a crystal ball that

would give us the ability to predict a violent crime before it occurred, however, we would have a much greater level of confidence in our ability to prevent it. Data mining gives us that crystal ball.

References

- Biskupic, J. (2011). Court strikes law restricting sale of prescription info. *USA Today*. June 23, 2011. Retrieved on July 29, 2011 from http://www.usatoday.com/news/washington/judicial/supremecourt/2011-06-23-supreme-court-prescription-data-mining_n.htm#
- Byrnes, J.D. (2002). *Before conflict: Preventing aggressive behavior*. Lanham, MD: Rowman & Littlefield Publishers, Inc.
- Ciarelli, N. (2010). How Visa predicts divorce. *The Daily Beast*, April 6, 2010. Retrieved on May 31, 2010 from <http://www.thedailybeast.com/blogs-and-stories/2010-04-06/how-mastercard-predicts-divorce/full/>
- Conley, L. (2009). How Rapleaf is data-mining your friend lists to predict your credit risk. *FastCompany.com: Where ideas and people meet*, November 16, 2009. Retrieved on May 31, 2010 from <http://www.fastcompany.com/blog/lucas-conley/advertising-branding-and-marketing/company-we-keep>
- Cook, R. (2011). Internet privacy not so private in court. *The Atlanta Journal-Constitution*. January 20, 2011. Retrieved on July 28, 2011 from <http://www.ajc.com/news/internet-privacy-not-so-809962.html?printArticle=y>
- Duncan, G. (2010). Zuckerberg: Online privacy is not a “Social Norm”. *Digital Trends*, January 11, 2010. Retrieved on July 28, 2010 from <http://www.digitaltrends.com/computing/zuckerberg-online-privacy-is-not-a-social-norm/>

EPIC (n.d.). Electronic Privacy Information Center. Retrieved on August 4, 2010 from

<http://epic.org/privacy/fusion>

Hof, R.D. (2009). Behavioral targeting: Google pulls out the stops. *Bloomberg Businessweek*,

March 11, 2009. Retrieved on July 28, 2010 from

http://www.businessweek.com/print/technology/content/mar2009/tc20090311_349208

Hylton, H. (2009). Fusion Centers: Giving cops too much information? *Time*, *March 9, 2009*.

Retrieved on August 4, 2010 from

<http://www.time.com/time/printout/0,8816,1883101,00.html>

Kaminski, R.J., Koons-Witt, B.A., Thompson, N.S., & Weiss, D. (2010). The impacts of the

Virginia Tech and Northern Illinois University shootings on fear of crime on campus.

Journal of Criminal Justice, 38 (1), pp. 88-98.

Kaufer, D. (2010). Right to absolute privacy on social media sites is “Wishful thinking”: Court.

Sophisticated Litigation Support Blog, *November 15, 2010*. [web log comment].

Retrieved on July 28, 2011 from

<http://www.sophisticatedlitigationsupportblog.com/2010/11/articles/social-networks/right-to-absolute-privacy-on-social-media-sites-is-wishful-thinking-court/print.html>

Sokolow, B.A., & Hughes, S.F. (2008). Risk mitigation through the NCHERM behavioral

intervention and threat assessment model. *National Center for Higher Education Risk*

Management, 2008 Whitepaper. Retrieved on July 28, 2011 from

<http://www.ncherp.org/pdfs/2008-whitepaper.pdf>

Sokolow, B.A., & Lewis, W.S. (2009). Second-generation behavioral intervention best practices.

Campus Law Enforcement Journal, *March/April 2009*, 39, (2), pp. 27-37.