3

Data Mining and Predictive Behavior

> That's the next great challenge for design: weaving the threats of technology, information, and access seamlessly and elegantly into our everyday lives. When a social network automatically checks us into a location, or cashiers can suggest new products based on purchase history, or our connected TV calls up our favorite shows when we walk into the living room…it may seem like magic.
>
> ~Scott Dadich, "The Age of Invisible Design" [1]

INTRODUCTION

In a book such as this that evaluates the effects of current trends on future actions and behaviors, the concept of prediction is at the core of each and every chapter. However, for this chapter, the focus and consideration of prediction shift away from macroconsiderations of prediction and focus more on the microcharacteristics of emerging technologies able to predict the behavioral choices of their users. In turn, the technology then responds in ways to anticipate those choices in advance and often without the awareness of the technological user. This type of technological functionality provides an extremely personalized experience with the information and providing technology, which ultimately is beginning to create similar expectations in broader applications—both within and external to the technology.

Before understanding the technological capabilities of predictive behavior, the concept of predictive modeling must first be considered. Predictive behavior modeling is the science of the application of mathematical and statistical techniques to historical and transactional data of customers to predict their future behavior [2]. By modeling future decisions, retention experts can make operational and resource allocation decisions that are more efficient and ultimately more effective than simply using historical examples to try to directly correlate into decision making. Put another way, IBM describes predictive modeling as having "the power to discover hidden relationships in…volumes of structured and unstructured data and us[ing] those insights to confidently predict the outcome of future events and interactions" [3].

From a marketing and business perspective, the benefits of predictive modeling and analysis are widespread. Specifically, this type of modeling typically has a positive impact on the optimization of existing processes, clarification of customer behavior, identification of unexpected opportunities, and anticipation of problems before they are impactful [4]. Likewise, it has routinely been shown to improve an organization's ability to up-sell products, cross-sell services, and improve customer retention campaigns as well as increase the relevance of the organization's communication processes with clientele [3]. Interestingly, even with the wide spectrum of potential positive impacts only 40% of organizations have partially or fully implemented predictive modeling strategies [4] (see Figure 3.1).

This type of modeling would be extremely beneficial to emergency management and public safety personnel. Given that these organizations (with rare exceptions) are hindered by limited resources, there is constantly a need to assess projects and programs to ensure that limited resources are prioritized effectively. Unfortunately, most emergency management organizations simply make planning, organizational, and resource management decisions based on a direct correlation to historical events and actions. The flaw with this technique is that it lacks the forecasting presence and predictive nature of discussed modeling. For example, public safety decisions made strictly on historical patterns would neglect the changing public expectations and communication strategies already discussed in Chapters 1 and 2, which clearly are altering future choices people make.

While there is no one single way to facilitate predictive modeling, there are some clear trends toward a few common approaches to this process. In most cases, the modeling methods require the quantification of risk based on all data, metrics, and measurements which can be collected about an individual user. This collection is often referred to as data mining,

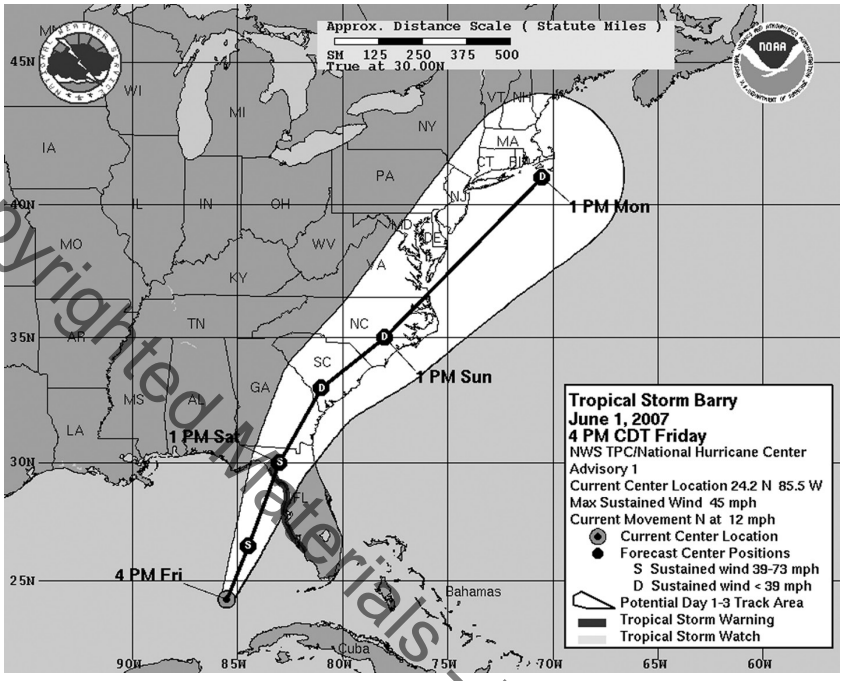

Figure 3.1 Predictive and forecasting technologies such as storm prediction tracks are often utilized, but other predictive technologies lack a similar level of usage. (Source: US National Weather Service.)

which has grown increasingly controversial in certain sectors like homeland security and national intelligence, but represents an extremely valuable and likely future application in all sectors within emergency management and public safety.

While data mining is highly complex and something that will most likely require professional support if fully leveraged in emergency management, the basics must be understood to begin to consider how it can be properly deployed now and in the future. In the simplest form, data mining is "the process of finding logical patterns in data and according order and meaning to various sets of seemingly random data" [5]. Other sources refer to these logical patterns as "knowledge," which is predictive modeling or the ability to take such knowledge and make accurate and discrete projections of future decisions and choices that may affect operational effectiveness or output [6].

The concept of data mining was first introduced in the 1990s, but has a long history tied back to classical statistics, artificial intelligence, and machine learning. The fundamental elements of data mining and ultimately predictive forecasting are a statistical evaluation including regression analysis, standard distribution, standard deviation, standard variance, discriminant analysis, cluster analysis, and confidence analysis [7]. However, this chapter will not consider these components in greater detail as they are unnecessary to understand at this interval. Instead, the possible applications of predictive modeling within disaster management operations will be the primary focus.

In a practical business sense, predictive modeling is widespread, but most often unknown to the end users. As a primary example, the vast majority of free online services, like e-mail or web browsing, are available at no cost due to the embedded information being gathered on the user's web browsing patterns, demographic data, purchasing choices, and search parameters (see Figure 3.2). Even though often unrecognized by the user, it is most evident in the sponsored advertisements, banners, pop-up messages, and other marketing tools that often appear immediately in response to browser actions. For example, if an Internet user utilizes a web browser to search for shoes, the next visited web page with embedded advertisements will promote available shoes, stores, deals, or other incentives to address the previously searched-for parameters. It is this

Figure 3.2 Data mining of free online services gathers browsing patterns, demographic data, and other information about the specific users. (Source: FEMA/ Marvin Nauman.)

automated and seemingly intuitive digital relationship that is often seen as predictive or "smart" in its application of a wide spectrum of data.

In Other Words…The Power of Data Mining

Data embodies a priceless collection of experience from which to learn. Every medical procedure, credit application, Facebook post, movie recommendation…and purchase of any kind—each positive or negative outcome, each successful or failed event or transaction—is encoded as data and warehoused. As data piles up, we have ourselves a genuine gold rush. But data isn't the gold—data in its raw form is boring crud. The gold is what's discovered therein. With the new knowledge gained, prediction is possible.

~Eric Seigel [8]

This phenomenon is also present within the digital tools utilized by many millions of people worldwide. For example, with more than 425 million active users, Google's Gmail system is widely utilized as a free e-mail service for people to send and receive e-mails with embedded and attached data. Because of the vast amount of information exchanged, Google aggregates the data and can provide embedded advertisements in response to words used within e-mails as a predictive modeling technology. For example, if an e-mail message contained references to a Native American name, Google might generate an advertisement relating to visiting Native American historical sites. [5,6].

While people certainly enjoy the possibilities of predictive modeling and behavior, there are concerns related to the process of the data mining necessary to achieve such activities. Specifically, the most significant concern related to data mining is the impact to both individual and collective privacy of the users of digital systems. This is particularly concerning if specific persons' names, aliases, social security numbers, e-mail addresses, bank account numbers, and other personal information are revealed via data mining; this leaves the possibility that private marketers, commercial companies, and/or government might utilize this information for unethical or nefarious purposes [9]. These types of ethical challenges related to the protection and preservation of an individual's personal data are the most significant potential hindrance

for the future of data mining with particular concern related to how government intelligence organizations have utilized and will utilize such data.

USING DATA MINING FOR INTELLIGENCE GATHERING

The US federal government utilizes data mining for a wide variety of programs. For example, according to one GAO survey, nearly 200 data mining efforts are underway by federal government agencies that seek out and leverage both personal and digital behavior data. Of those identified, nearly 35% were directed at service improvement or performance programming, 12% targeted fraud and waste detection, 11% analyzed scientific and research information, and an additional 8% were used to detect criminal activities and behaviors [9]. It is this last characteristic that has the widest implications on public safety, homeland security, intelligence, and emergency management functions now and into the future.

For example, the Markle Foundation's Taskforce on National Security in the Information Age stated that "information analysis is the brain of homeland security… [if] used well, it can guide strategic, timely moves throughout…the world… [and if] done properly, even armies of guards… will be useless" [10]. Specifically, collecting and analyzing all available data under predictive modeling is far more reliable, accurate, and valuable than simple linear associations in the field of homeland security. For example, identifying a connection between individual suicide bombers and religious extremism adds little value to an organization's ability to combat terrorism, but making connective predictions would increase the likelihood that information about the when, where, and how of planned terrorist events may occur [10]. While nearly all intelligence organizations handle and process data mining at some level, the US National Security Agency (NSA) is one of the most well-known and notorious agencies utilizing these capabilities (see Figure 3.3).

The criticality of data mining and predictive behaviors for national intelligence systems increased in its importance after the terrorist attacks on September 11, 2001. This change in relevance was absolutely critical given the highly decentralized approach of the terrorists responsible for the attacks. Specifically, terrorist cells were both independent and connected, as well as spread throughout the world with minimal use of complex systems and often in the process of long-standing preparations for the assigned tasks. Additionally, the information systems and data

Figure 3.3 The US National Security Agency (NSA), as well as numerous other governmental agencies, has been given the authority to use data mining to gather and leverage user information for various reasons. (Source: FEMA/Bradley Carroll.)

exchanged in these decentralized cells often leveraged the full complexity of digital technology. For example, anonymous e-mail accounts or pay-as-you-go (also known as "burner") mobile phones were leveraged to send, receive, and ultimately act on such information. Consequently, without data mining, it became abundantly clear that it was nearly impossible to detect, collect, analyze, and ultimately decipher nefarious information from terrorists when it was simply buried in nearly 2.5 quintillion bytes of other data exchanged every day [11].

Consequently, intelligence organizations like the NSA quickly moved to expand data mining processes to help more clearly establish connections between people and information. These systems quickly began to put filters or aggregators on information to—in essence—force the astronomical amount of data into measurable "pipe" information where the patterns and connectivity could begin to be seen. In other words, as the data-mining saying goes: "To find a needle in a haystack, you need to first build a haystack" [12]. The building of the so-called digital haystack most frequently relies on extra data that are added as a "tag" onto the primary data. These tags are called metadata and help allow commercial companies and ultimately intelligence organizations to search and filter

in order to pull desired data or behavior patterns. Interestingly, metadata tags have a murky legal status when compared to traditional or direct communication methods. For example, the NSA (or other government intelligence-gathering organizations) cannot examine the communications of a US citizen or resident alien, but there are no such limitations on an individual's metadata [11].

The use of metadata to collect information and predict future behavior is ostensibly to prevent future terrorism or other acts that impact public safety. Unfortunately, this process is intentionally wrapped in subterfuge to prevent the public from knowing the process and ultimately finding a way to circumvent the detection. For example, China's Public Security Bureau adds additional goals of public opposition to government leaders and minimizing public opposition to government decisions and operations [12]. Under any approach, the public provides information to the proverbial equation, but has no engagement and little choice in the process. The ubiquitous nature of digital systems and corresponding devices makes avoidance of "digital haystacks" extremely difficult for the average user. Consequently, when a former American government intelligence analyst named Edward Snowden released classified information about data-mining systems in June 2013, the world took notice and began to question the processes and appropriateness of these systems.

Specifically, Snowden took nearly 200,000 classified documents that he had access to and fled to Hong Kong and later Russia. Snowden quickly released the documents to the traditional media in various international markets, who began to identify and analyze information about the inner workings of the US intelligence community. For example, traditional media outlets quickly identified that the NSA collected records of every American phone call under a call log metadata program. Moreover, the *Washington Post* revealed that the NSA infiltrated the cloud-based services of Google and Yahoo to collect the data of America's digital profiles and activities. Other European media outlets determined from Snowden's released documents that the United States collected data on allies, including Germany, France, and Italy [13].

Additionally, a Snowden-leaked document revealed an NSA surveillance program called US-984XN, which was more commonly known by its code name, PRISM, which was established by President George W. Bush in 2007 as a covert program for warrantless domestic surveillance (see Figure 3.4). PRISM involved the collection of digital photos, online storage data, file transfers, e-mails, chat room logs, videos, and video conferencing data from nine major American Internet companies [11].

Figure 3.4 US President George W. Bush initiated a covert digital surveillance program in 2007 which was further developed under President Obama and later revealed by NSA whistleblower Edward Snowden. (Source: White House/Eric Draper.)

Specifically, through PRISM, the NSA was able to extract information directly from the servers of companies like Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, and Apple [14]. Likewise, it was quickly confirmed that the Government Communications Headquarters (GCHQ; Great Britain's equivalent to the NSA) had also been secretly data mining information from the same Internet companies through an operation set up by the NSA. Specifically, this NSA-generated system would allow GCHQ to circumvent the formal legal process required in Great Britain to collect personal information included in e-mails, photos, and photos from Internet companies based outside the United States [14].

The challenge is that these systems are not foolproof. The effectiveness and appropriateness of these systems must be taken in balance when considered against the impacts to privacy and questions related to legal and ethical application of data mining. Well before Snowden released the classified documents, many information security experts were already questioning the effectiveness of data mining on the identification of terrorists and the prevention of future acts of violence. For example, in a 2007 sworn testimony to the Committee on the Judiciary of the United States Senate, security experts stated that "with a relatively small number of [terrorist] attempts every year and only one or two major terrorist incidents every few years—each one distinct in terms of planning and execution—there are no meaningful patterns that show what behavior indicates planning or preparedness for terrorism" [15]. Likewise, routine and acceptable behavior of the general population can lead to its misidentification as

questionable behavior. For example, after the September 11 terrorist attacks, many government leaders and emergency response organizations questioned (and even arrested) individuals for taking pictures of bridges, monuments, and buildings (see Figure 3.5). While this behavior may be used for nefarious purposes, it is much more likely a pattern of innocent behavior related to tourism or hobby photography, for example [15].

Regardless of these limitations, concerns, and political and public black eyes, intelligence organizations are continuing to move forward with the dedication of resources, personnel, and procedures to the use of data mining for homeland security and terrorism prevention. For example, the NSA is building a $1.7 billion facility in Utah that will facilitate the storage and processing of data-mining information and related classified information. This facility will be the largest data storage center in the United States and will constantly use 65 megawatts of electricity, which is enough to power 33,000 houses. The NSA is maintaining a high level of secrecy related to the facility and will not reveal any specifics about the operations or structure of the location [16]. This facility was initially

Figure 3.5 After 9/11, there was a significant concern about individuals who took pictures of bridges, monuments, buildings, and other pieces of critical infrastructure. (Source: US Navy/Sgt. Andy Dunaway.)

welcomed by politicians in Utah with a promise that activities would be "conducted according to constitutional law," but many national leaders in as many as 10 states have introduced legislation to limit or withdraw funding to support this effort [16]. The challenge of the commitment and possible uses of data mining by the NSA most likely will continue to run contradictory to public and political pressure until a balance of privacy and protection can be found.

PUBLIC SAFETY USES OF DATA MINING AND PREDICTIVE MODELING

National homeland security and intelligence organizations are not the only groups using data mining and predictive modeling. Law enforcement entities at the local, state, and federal levels of government are beginning to utilize and consider future applications of these technological capabilities. Much like the intelligence communities already mentioned, law enforcement organizations are burdened by a similar amount of data that can quickly overwhelm professional analysts without data mining and predictive modeling possibilities.

The use of data mining and predictive modeling in law enforcement is a relatively new concept. Back in 2009, seven American police organizations received planning grants through the National Institution of Justice's (NIJ) competitive solicitation process to consider how digital information could be collected and analyzed to prevent and/or reduce crime in various communities. These organizations included police departments from large metropolitan areas including Los Angeles, Boston, Chicago, New York, and Washington, DC [17]. These entities and many since have begun to utilize predictive policing in four major areas: predicting crimes, predicting offenders, predicting the identity of perpetrators, and predicting victims of crimes. Predicting crimes is the broadest of these categories and focuses on the forecasting of places and times that have an increased risk of crime. Similarly, other models attempted to predict the identity of individuals at increased risk of committing crime in the future. The identity of perpetrators can also be projected against certain profiles that can more accurately predict likely offenders with specific past crimes. The last and perhaps most interesting classification model being utilized is related to the prediction of victims of crimes. In all four cases, leveraging these types of models could potentially have a significant impact on public safety and clearly is becoming commonplace and will likely become

a best practice across all types of organizations as resources and comfort with technology become more available [18].

Much like the intelligence community utilization of predictive modeling, there are limitations related to how law enforcement can effectively use these systems. For example, some people have argued that effective predictive crime simply displaces the crime to another geographic area or jurisdiction. However, these types of challenges are often countered in the algorithms utilized in the data processing and/or create a halo effective by having positive, yet unintentional, impacts on other areas [19]. Additional limitations include an over-reliance on predictions and/or erroneous data. For example, some law enforcement agencies lack effective strategies to transition from the predictions to tactical application to actually stop or reduce crime in the area. Likewise, if erroneous data or related assumptions are applied, the predictions applied to the collected data can lead to misapplied resources and ultimately reduce the impact of reducing crime or the effectiveness of overall public safety initiatives [18].

PERSONAL PREDICTIVE BEHAVIOR

Predictive behavior technology is not limited to professional and widespread uses in public safety and emergency management. Many newer digital systems and mobile technologies such as cell phones and tablet computers have embeddable technology (or applications) that serve as so-called virtual personal assistants. Examples of these virtual personal assistants include Siri by Apple, Google Now, Mynd, and Cortana by Microsoft. In most cases, these software programs are voice activated and respond to requests made by the user (e.g., location of building, message generator, etc.). While impressive in their own right, these systems are also ultimately designed to recognize patterns and design in the behaviors of the device user.

These prediction-based virtual personal assistants have and will continue to grow in importance as various forms of emerging and disruptive technologies integrate with various mobile devices (see Chapter 4). Consequently, companies like Apple, Google, and Microsoft will continue to invest in the capability and reliability of these systems. As they improve the capabilities and streamline these potential integrations, the possibilities for these systems for respective public safety and emergency management personnel and organizations are vast. While operational applications are still limited given the minimal amount of data

available in most communities (i.e., the lack of emergencies and disasters personally handled by staff), the day-to-day applications are far more promising. Using predictive technologies embedded in mobile phones or tablets to cut down on the device recall for work schedules, operational conditions (e.g., weather), task reminders, and automated messages will ultimately improve the efficiency and effectiveness of individual practitioners.

In Other Words…Expectations of Predictive Technologies

How could there be anything wrong with this conventional design paradigm? Functionality? Check. Content? Check. Customer personas? Ah—herein lies the problem. These aggregate representations of your customers can prove valuable when designing apps and are supposedly the state of the art when it comes to customer experience and app design, but personas are blind to the needs of the individual user. Personas were fine in 1999 and maybe even in 2009—but no longer, because we live in a world of 7 billion "me's." Customers increasingly expect and deserve to have a personal relationship with the hundreds of brands in their lives. Companies that increasingly ratchet up individual experiences will succeed. Those that don't will increasingly become strangers to their customers.

~Mike Gualtieri, Forrester Blogs [20]

However, like the data mining and broad-scale predictive behavior mentioned earlier in the chapter, the personal uses of these technologies also have limitations and ethical concerns regarding deployment. For example, whether the mobile device is on-demand (e.g., Siri) or in a state of constantly listening (e.g., Google Now), the device is constantly monitoring, collecting, and processing personal information ranging from location to online searching patterns. This type of technology can create "Big Brother" ethical and privacy concerns [20]. Each software developer and device designer will have to address this privacy issue in ways that are consistent with the product and brand management (similarly to the large-scale balance mentioned earlier). For example, Microsoft's Cortana project has a built-in dashboard to allow users to see exactly what information the software is tracking and the types of data being saved [21].

SHIFTING TOWARD SMART BEHAVIORS

Businesses are utilizing data mining and related mathematical algorithms to collect and aggregate customer (or potential customer) activities into predictable or measurable behaviors. Because customers do not directly engage in these activities and frankly are often unaware they are occurring, there is a tremendous spectrum of possible uses and impacts. These measurable behaviors are being leveraged to create organizational opportunities that can increase profit, improve client experience, and strengthen customer service. Likewise, as will be discussed in this section, there are also significant potential implications on how this type of behavior can potentially be used to influence the behavior of individuals before, during, and after disasters.

For example, the Target organization assigns every customer an identification number that is tied to credit card numbers, purchasing history, e-mail addresses, personal mailing address, and other personal data. Once these are collected Target often looks to send targeted coupons and other marketing material via mail or e-mail. For example, Target sends coupons to women who appear (via predictive behavior) to be pregnant or trying to conceive. After analyzing years of purchasing data of pregnant women, Target administrators determined that women on the baby registry purchased larger quantities of vitamin supplements (e.g., calcium) in their first trimester, unscented lotion at the beginning of their second trimester, and cotton balls and hand sanitizers just prior to their delivery date (see Figure 3.6). Target utilized these product-purchasing patterns as well as those for 22 other products to create a "pregnancy prediction" score which was then used to trigger targeted coupons and other promotional materials. In the end, Target's revenue from pregnant (or trying to get pregnant) women grew from $44 billion in 2002 to $67 billion in 2010 due to the data-mined process of "heightened focus on items and categories that appeal to specific guest segments such as mom and baby" [22].

Online retailer Amazon is also attempting to potentially leverage customer behavior patterns to reduce shipping time for their customers. According to an Amazon patent filed in 2014, the company is attempting to utilize previous orders, system searches, wish lists, and cursor hovering time to create "anticipatory shipping" where the products bought by the customer start traveling to the nearest shipping hub before a purchase button has been clicked [23]. While Amazon's predictive shipping model is only a theory at the time of print, it is a strong indicator that private

Figure 3.6 Target infamously utilized data mining to create predictive modeling around how pregnant women would buy goods and products. (Source: FEMA/ Liz Roll.)

companies have sought and will continue to seek out ways to predict behavior to improve operational processes and ultimately the financial impact to the organization.

Although still not commonplace, these sorts of predictive behavior models are being directly utilized to improve community and individual health, safety, and emergency preparedness. For example, in 2014, Google announced the $3.2 billion acquisition of a company called NEST Labs, which is a maker of home automation equipment such as thermostats and smoke/carbon monoxide detectors. Since 2011, NEST has made products that are "smart" and ultimately learn from the behaviors and choices of the end user. For example, the thermostat is programmable (like any other thermostat), but the NEST products learn desired temperatures and raise or lower the temperatures based on occupancy patterns (e.g., workday vs. weekend) in the area, which ultimately improves energy efficiency and lowers costs [24,25]. Likewise, the "smart" smoke and carbon monoxide detector responds to safety risks with a human

voice and a "friendly heads-up" that includes information about in which room the smoke or carbon monoxide is located [24]. The devices also constantly monitor battery life and send messages to a smartphone app when they need to be replaced, which is both more efficient and less arbitrary and impactful than currently recommended preparedness strategies [26]. While this type of predictive modeling system is not without integration challenges, it yet again shows a shift toward processes that allow for and support the use of past behaviors to predict future choices and activities.

LEVERAGING EMOTIONAL CONNECTIONS

One of the strongest possible benefits of using data mining and predictive modeling for business and commercial practices is the possibility of eliminating hurdles for the consumer and thus providing a completely positive experience with the brand or product line. These types of positive experiences create emotional connections (positive or negative) and ultimately can further be leveraged for long-term brand connectivity and loyalty. Specifically, organizations will utilize emotional branding to appeal to a customer's emotional state, ego, desires, and needs [27]. When these emotion-based characteristics are leveraged, consumers often engage in a self-fulfilling prophecy of consumer engagement. Brands like Nike and Timberland create emotional stories and narratives (see Chapter 2) around consumer experiences by creating heroes or lifestyles around those individuals to whom, ultimately, the consumer is emotionally attached or wishes to emulate [27].

While some consumer groups have objected to all forms of emotional branding as manipulative of human emotions, it is important for public safety and emergency management professionals to understand the power of putting local citizens or a broader constituency in positive emotional positions to make more effective and predictable decisions before, during, and after a disaster. This emotional attachment is why many emergencies or disasters are defined by an emotional photo, video, or narrative of people uniquely impacted by the event. This emotional connection also drives fund-raising initiatives, donations management, and volunteerism rates during certain events. If this concept is more broadly understood, it may be possible to leverage it for expected behaviors and actions during emergencies or disaster recovery activities.

REFERENCES

1. Dadich, Scott. (2013). "The Age of Invisible Design." *Wired*. September/October 2013.
2. "Predictive Behavior Modeling." (2013). Optimove Learning Center. http://www.optimove.com/learning-center/predictive-behavior-modeling. Accessed April 25, 2014.
3. "Predictive Modeling." (n.d.). IBM. http://www-01.ibm.com/software/analytics/solutions/predictive-modeling. Accessed April 25, 2014.
4. Eckersen, Wayne W. (2007). "Predictive Analytics: Extending the Value of Your Data Warehousing Investment." The Data Warehousing Institute. http://www.sas.com/events/cm/174390/assets/102892_0107.pdf. Accessed April 25, 2014.
5. Saitta, Sandro. (2010). "What Is Data Mining?—Explaining It to the Layman." *Data Mining Research*. http://www.dataminingblog.com/guest-post-what-is-data-mining-%E2%80%93-explaining-it-to-the-layman/. Accessed April 27, 2014.
6. Ludwig, Sean. (2012). "Gmail Finally Blows Past Hotmail to Become the World's Largest Email Service." *Venture Beat News*. http://venturebeat.com/2012/06/28/gmail-hotmail-yahoo-email-users. Accessed April 29, 2014.
7. "Data Mining." (n.d.). University of North Carolina. http://www.unc.edu/~xluan/258/datamining.html. Accessed April 27, 2014.
8. Wolverton, Joe. (2013). "Predictive Analytics: The Power to Predict Human Behavior." *The New American*. http://www.thenewamerican.com/reviews/books/item/15660-predictive-analytics-the-power-to-predict-human-behavior. Accessed April 26, 2014.
9. "Think Before You Dig: Privacy Implications of Data Mining and Aggregation." (2004). NASCIO. http://www.nascio.org/publications/documents/nascio-datamining.pdf. Accessed April 30, 2014.
10. McCue, Colleen. (2005). "Data Mining and Predictive Analysis: Battlespace Awareness for the War on Terror." *Defense Intelligence Journal*. 13-1&2. http://innovative-analytics.com/docs/BattlespaceAwarenessDIJ.pdf. Accessed April 26, 2014.
11. Pappalardo, Joe. (2013). "NSA Data Mining: How It Works." *Popular Mechanics*. http://www.popularmechanics.com/technology/military/news/nsa-data-mining-how-it-works-15910146. Accessed May 1, 2014.
12. Harrison, Mark. (2013). "Needles in the Mega-Haystack: NSA Versus KGB." Warwick Centre on Competitive Advantage in the Global Economy. http://blogs.warwick.ac.uk/markharrison/entry/needles_in_the. Accessed May 1, 2014.
13. Kelley, Michael and Nudelman, Mike. (2013). "The Snowden Saga: Here's Everything We Know about the NSA's Nightmare Leak." *Business Insider*. http://www.businessinsider.com/everything-we-know-about-snowden-leaks-2013-11. Accessed May 1, 2014.

14. Gellman, Barton and Poitras, Laura. (2013). "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *The Washington Post*. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Accessed April 1, 2014.
15. Harper, Jim. (2007). "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs." Cato Institute. http://www.cato.org/publications/congressional-testimony/balancing-privacy-security-privacy-implications-government-data-mining-programs. Accessed May 2, 2014.
16. "Electrical Problems Put Damper on NSA's Secretive New $1.7 Billion Data Center in Utah." (2013). *NY Daily News*. http://www.nydailynews.com/news/national/nsa-center-utah-plagued-eletrical-issues-article-1.1479845. Accessed May 2, 2014.
17. "Predictive Policing Symposium: Discussion on the Predictive Policing Demonstration Projects and Evaluations." (2012). National Institute of Justice (NIJ). http://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/symposium/Pages/discussion-demonstrations.aspx. Accessed May 2, 2014.
18. Perry, Walter L. (2013). "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations." RAND Corporation. https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf. Accessed May 2, 2014.
19. Groff, Elizabeth R. and Lavigne, Nancy G. (n.d). "Forecasting the Future of Predictive Crime Mapping." *Crime Prevention Studies* 13:29–57. http://www.popcenter.org/library/crimeprevention/volume_13/03-groff.pdf. Accessed May 2, 2014.
20. Gualtieri, Mike. (2013). "Predictive Apps Are the Next Big Thing in App Development." Forrester Blogs. http://blogs.forrester.com/mike_gualtieri/13-08-28-predictive_apps_are_the_next_big_thing_in_app_development. Accessed May 3, 2014.
21. Covert, Adrian. (2014). "Google Now and Cortana Are the Future, Not Siri." *CNN Money*. http://money.cnn.com/2014/04/28/technology/innovation/google-now-cortana-siri. Accessed May 3, 2014.
22. Hill, Kashmir. (2012). "How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did." *Forbes*. http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did. Accessed May 6, 2014.
23. Sorokanich, Robert. (2014). "Amazon Might Try Shipping Things Before You Even Buy Them." Gizmodo. http://gizmodo.com/amazon-might-try-shipping-things-out-before-you-even-bu-1503661403?rev=1389991970&utm_campaign=socialflow_gizmodo_twitter&utm_source=gizmodo_twitter&utm_medium=socialflow. Accessed May 6, 2014.

24. Curtis, Sophie. (2014). "What Is NEST and Why Has Google Bought It?" *The Telegram*. http://www.telegraph.co.uk/technology/google/10570414/What-is-Nest-and-why-has-Google-bought-it.html. Accessed May 6, 2014.
25. Turrentine, Lindsey. (2014). "Second-Gen NEST Zeroes in on Perfection." CNET. http://www.cnet.com/products/nest-learning-thermostat. Accessed May 6, 2014.
26. "Life with NEST." (n.d.) NEST Labs. https://nest.com/smoke-co-alarm/life-with-nest-protect. Accessed May 6, 2014.
27. Barakat, Christine. (2014). "Emotional Branding and the Emotionally Intelligent Consumer." Social Times. http://socialtimes.com/emotional-branding-emotionally-intelligent-consumer_b140449. Accessed May 7, 2014.