Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, August 2016, vol. 21, no. 2

THE LESSONS OF INTERNET BANKING, BIO-SURVEILLANCE AND PREDATORY LOAN PRACTICES

JEFFREY E JARRETT

University of Rhode Island, Management Science and Finance, USA, Tel: +401-874-4169;

Email: **jeffreyejarrett@gmail.com**

Abstract

Internet banking is a rapidly growing industry which includes all financial institutions, lending and similar institutions that implement financial savings, and borrowing, insurance and similar functions. With the growth comes problems that can be illustrated, solved and improved by data analytics originally produced to solve problems in industrial experimentation, quality control and continuous improvement. This is particularly important in industries that are largely unregulated and involve free markets. By utilizing the experience in health and medical care, we exemplify how data analytics changed and improved analysis in an industry other than industrial production and experimentation. These analytics will improve the functioning of internet banking and similar industries.

INTRODUCTION

One of the difficult problems in delivery of product from retailer to end-user customers. There are similar problems in the delivery of product from a manufacturer to the next point on the line from manufacturer to end-user customer [1]. Commercial products are not the only transfers of information but include transporting of product that cannot be delivered on-line. This problem, called logistics is age old but is referred to in modern vernacular as the “supply chain.” Usually, supply chain problems and its industry refer problems of delivery of end-products or supplies. In previous studies of internet banking and ecommerce, we found that internet communication serves as an extremely useful in the fields of ecommerce and internet banking. The difference here was being that the communication systems provide the information system with the ability of communicating vital data to transfer quickly and accurately from sources of information to the end-users of this information.

APPLICATION TO THE PREVENTION OF DISEASE AND EPIDEMICS

Previous studies of the use of data analytical quality control methods indicated that the results of scientific testing of patients and those engaged in controlled subjects in scientific experiments require the use of the latest scientific methods from statistical analysis. No longer do medical, health and prevention of plagues, viruses, epidemics and new drug treatments require only a simple test of hypothesis to determine future actions to prevent the negative outcomes of health analytics. Unusual results can still occur but the latest data analytics can postpone the introduction of new drugs, treatments before diagnostic failures cause additional problems. Speed is important and backing of good legislation by authorities is crucial in setting up programs. The postponement of decisions naturally may impose additional costs to society which do not enter the income statements of non-socially desirable activities. As an example the continuation of fracking may increase the supply of heating and energy sources but costs of such activities may be non-beneficial to the future activity of our planet.

The idea of ignoring future evidence that a natural disease outbreak may occur diminishes the importance of the utility of a bio-surveillance program and whether during an influence or Zika or Ebola virus outbreak, the system should still be looking for a bio-terrorism attack. If the overriding goal is the detection of criminal terrorism, then silencing the detection procedure during a virus season could have terrible consequences to a desirable outcome. Furthermore, if that is the goal, then during a natural disease outbreak the Bio-surveillance systems may likely require modifications to better detect criminal terror attacks using biological methods.

By employing data analytical methods based on, for example, adaptive multi linear regression with a sliding baseline may improve the processes of detection. If such a method is simply automatically implemented, as analysts are able to do, then an attack that occurs during a natural disease outbreak will be very difficult to detect. Detection will be difficult and doubly difficult when a long sliding baseline produces redundant

signals in choosing treatments. These results after the disease outbreak will be indistinguishable from the signals related to a criminal attack using biological processes.

Furthermore, the best method to attempt to identify a criminal attack when an outbreak is occurring is to adjust the sliding baseline of the adaptive regression so that it only includes data from the outbreak period. If the outbreak is long enough that a newly established sliding baseline may produce improved results. At that time, one can use the system signal that indicates an additional departure from the outbreak. However, If that is the case, then the bio-surveillance system will be of necessity require as a model that requires human interaction to identify the start of the influenza or virus season and to adjust the adaptive regression model to produce a sliding baseline that only diagnoses the influenza or virus outbreak data.

CAN ONE AUTOMATE A BIO SURVEILLANCE SYSTEM ON-LINE?

While there is significant interest in the research and public health communities in devising automated methods of detection capable of sifting through masses of data to identify outbreaks and bioterrorism attacks, research will lead decision and management science to conclude that, at least for the foreseeable future, that detection algorithms alone will not be sufficient and human-in-the-loop methods will be required for effective detection [2]. The use of internet connections and supply chain of information will require human-in-the-loop connections. As an example, the implementation of adaptive regression models can be improved with the application of human judgment. As just described, if the purpose is bioterrorism detection, then the baseline should be adjusted to the extent feasible during natural disease outbreaks to make bioterrorism detection possible during such outbreaks. This can only be done by a human making an informed decision about when the outbreak started. In a related situation, if the goal of a bio surveillance system is to detect departures from the natural background disease incidence, then the performance of the adaptive regression immediately after an outbreak will be improved by removing the outbreak data from the sliding baseline. Thus, if one includes the outbreak data would result in impaired analysis and the accurate estimation of predicted values immediately following the outbreak would be imperfect. This again will require a human making an informed decision about both when an outbreak started and when it ended. Last, we note that simply allowing an adaptive regression to automatically proceed sequentially through bio surveillance data without removing outbreak data (as we allowed out of convenience can result in false signals. This can occur when, for example, the sliding baseline consists mainly of the data during the period when an outbreak is subsiding, such that the slope of the regression is negative. Under this condition, if there is an abrupt return to the normal condition, then it is possible for the adaptive regression to under-predict, resulting in positive residuals and an alarm condition. Simply put, to the adaptive regression methodology, a sudden increase from the background disease incidence pattern looks the same as a sudden leveling off from an outbreak returning back to a normal condition. And, while one might be tempted to not allow signals in the case of the slope of the adaptive regression is negative. The result would be to also prevent the

procedure from detecting outbreaks or attacks during periods when there are even slight improvements in disease incidence.

Note, we are restricting this discussion on the application of adaptive regression; the underlying issues are broader and not limited to just adaptive regression-based methods. This suggests that improvements in the practice of bio surveillance will continue to require advances in detection algorithms combined with development of detection algorithm practices and procedures as defined over time by experienced bio surveillance system operators and enhancements in bio surveillance system software capabilities. Most interesting is the use of data management systems to assist adaptive data analytics to prevent outbreaks of epidemics, bioterrorism and influenza attacks from general populations.

THE APPLICATION TO INTERNET BANKING AND PERSONAL BANKING

All of the above methods that are not being applied in bio surveillance can now be applied to internet banking and the similar operation in personal lending as exemplified by the “Lending Club.” The latter title is now referred to many operations in which borrowers engage in activities to secure loans by personal means often through internet services. Consumer protection in these operations is vulnerable to aspects of predatory lending practices. Largely these practices are not regulated or only slightly regulated and give rise to and lead to enormous penalties on the part of the consumer borrower who is often unaware or not sophisticated enough to understand the ramifications of the process. These include not only second mortgages and consumer loans but in particular loans associated with higher education.

Consumers protect laws in general have not kept up with the infusion of the internet into the borrowing and lending functions of financial institutions [banks; non-bank financial intermediaries; and personal lending operations]. They prey on the vulnerable that often include the aged, higher education students, the less educated and others who are unprotected from operations designed to be predatory. In the state of New Jersey, for example, if a higher education student somehow defaults on loans and dies, the loan may still have to be paid by his relatives (parents) and this is backed by state law. This would include the garnishing of assets, income or others including the non-payment income tax rebates to the parent in the action. Hence, the state by holding the parent liable is by all means an action that may very well be thought of as “predatory.”

Much of the actions of lenders can be predicted analyzed by consumer protectors authorized by statute to implement such protection. Analytically examining of determining faults in the borrower-loaner actions can use the principles of data analytics to determine who is at fault in the system. Multivariate quality or process control originally developed in the field of industrial quality and management can aid in the prevention of fraud, predatory actions and other forms of actions to aid in the protection of consumers in their loan activity.

SUMMARY

We developed the argument that applications of industrial quality control and data analytics have unusual applications in fields far and distant from their original applications. They include the great development of diagnostic tests, disease prevention and other applications in the fields of health and medical care. There is a special set of need in the protection of borrowers in internet banking operations including personal lending that need to be examined and resulting in consumer protection. There is a place for data analytics and application of industrial quality control in this field that can determine practices that are predatory and designed without scruples. In the future, we expect that many of these practices will be examined and eliminated. The internet banking establishment should be cognizant of all this and determined to stop illegal and predatory operations. Remember “Red Lining” is gone and so are many other immoral operations.

REFERENCES

1. Schneier B (2015) The Hidden Battles to Collect Your Data and Control Your World. Data and Goliath, London.
2. Warren E (2014) Fighting Chance. Holt, New York.