Big data: from marketing to safer streets

Can commercial big data improve pre-crime analytics?

by Stephan D. Hofstetter

***Stephan D. Hofstetter** is founder and managing partner of SECOIA Executive Consultants Ltd. He has professional experience in various fields of security document systems, mission command and crisis management. He holds degrees in international security studies, business administration and media engineering. He is passionate about linking industries and specialised firms to governmental use cases, thus creating next-generation solutions and success for all stakeholders involved.*

Intelligence-led policing has been around since the 1990s, but as elements such as profiling are still controversial and there are no universally established procedures for acting on the intelligence, success has been limited. In the private sector, big data has been successfully used in precision marketing and credit risk analysis. Ethical and legal constraints have been limiting governments in their use of predictive methods while commercial options seem rather 'open-sky' in comparison. Anonymised data collected by the private sector could be used to enhance models of criminal projections. How predictive analytics can improve crime prevention has therefore become the subject of a study.

The issue

While intelligence-led policing is an important topic and field of ongoing research within the various police units, the introduction, application and response are still in an experimental stage. Intelligence-led policing "is a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem-solving, which the field has considered beneficial for many years."[1] In recent years, governments' expectations regarding successful policing and crime prevention have increased. Recent terror attacks have further increased the pressure on police forces and internal and external migration have affected the social cohesion of communities and the wider society.

Intelligence-led policing spans many disciplines such as pre-crime analytics, neighbourhood policing and profiling. The United States has taken a leading role in this field, partially due to the liberalisation of their legal framework in the aftermath of the 9/11 attacks. Later, this led to the introduction of the biometric-electronic passport and border control, and most recently to the passing of the CLOUD Act on 23 March 2018 by the current administration.[2] Use cases in Switzerland and the Netherlands as well as relevant studies in Europe show a preference for methods based on pattern observations of localised crime incidences.

The 'near repeat' theory

Typological profiling is a long-standing, well-documented and controversial field of science within the police and success is viewed with caution. It focuses on typology of individuals who fit an identified or assumed pattern. It is very much human-oriented. One of the frequently discussed methods is the 'near repeat theory'. It is based on two main principles. The first is the likeliness that a criminal will repeat delicts he has been successful with. The second is that a victim or particular area is likely to be targeted again in the near future. Today, predictive analytics is focused on patterns of repetition in incidences, sometimes enhanced with environmental factors and psychological observation of local criminals.

While prediction is a useful instrument for policing, in order to prevent crime, action must be taken. However, there are no established procedures for acting on the intelligence gained or measuring the success of these actions. Both are still the subject of ongoing research.

Impacting behaviour through big data

An entirely different discipline, which is also about predicting and actually influencing human behaviour is marketing, and in particular consumer marketing. Fundamental to this is big data. Big data is a buzz word used to refer to many things, ranging from aggregating data on an enormous scale to actual methodologies of aggregating, storing, processing and gaining intelligence from the data. Big data enables marketeers to go beyond the 'dump pipe' of promoting products using conventional marketing methods. Marketing traditionally focuses on human behaviour and linking this to an incidence, usually a purchase. It is then evaluated which factors affect the likelihood of an individual making that purchase.

Several business cases justify this thought i.e. South Korean Telecom (SK Telecom) combines in-house data, with social network data and creates customer profiles that enable their internal marketing department and their business customers to execute their precision

marketing strategies. This involves customised offerings, communication and business models tailored to each customer. Personalised profiling is also used in financial applications: credit providers use big data to assess the creditworthiness of individuals and businesses.

Limitations of pre-crime analytics

The current methodology of pre-crime analytics is very much regionalised and it often fails to consider organised crime that spans a wider geographical area. It operates similarly to merchants with a local customer base. They are successful in their local market because they know their customers and how they are influenced. When they receive potential customers from other areas, these are not reached, understood and managed. Predictive methods in marketing rely on individually profiled persons, geotagged and monitored using the localisation features of various apps. In order to adhere to the legal framework, tracked individuals must have knowingly or unwittingly consented to these methods. There are many success stories in which predictive behaviour was combined with location, or in which irregularities were analysed and used for marketing purposes.

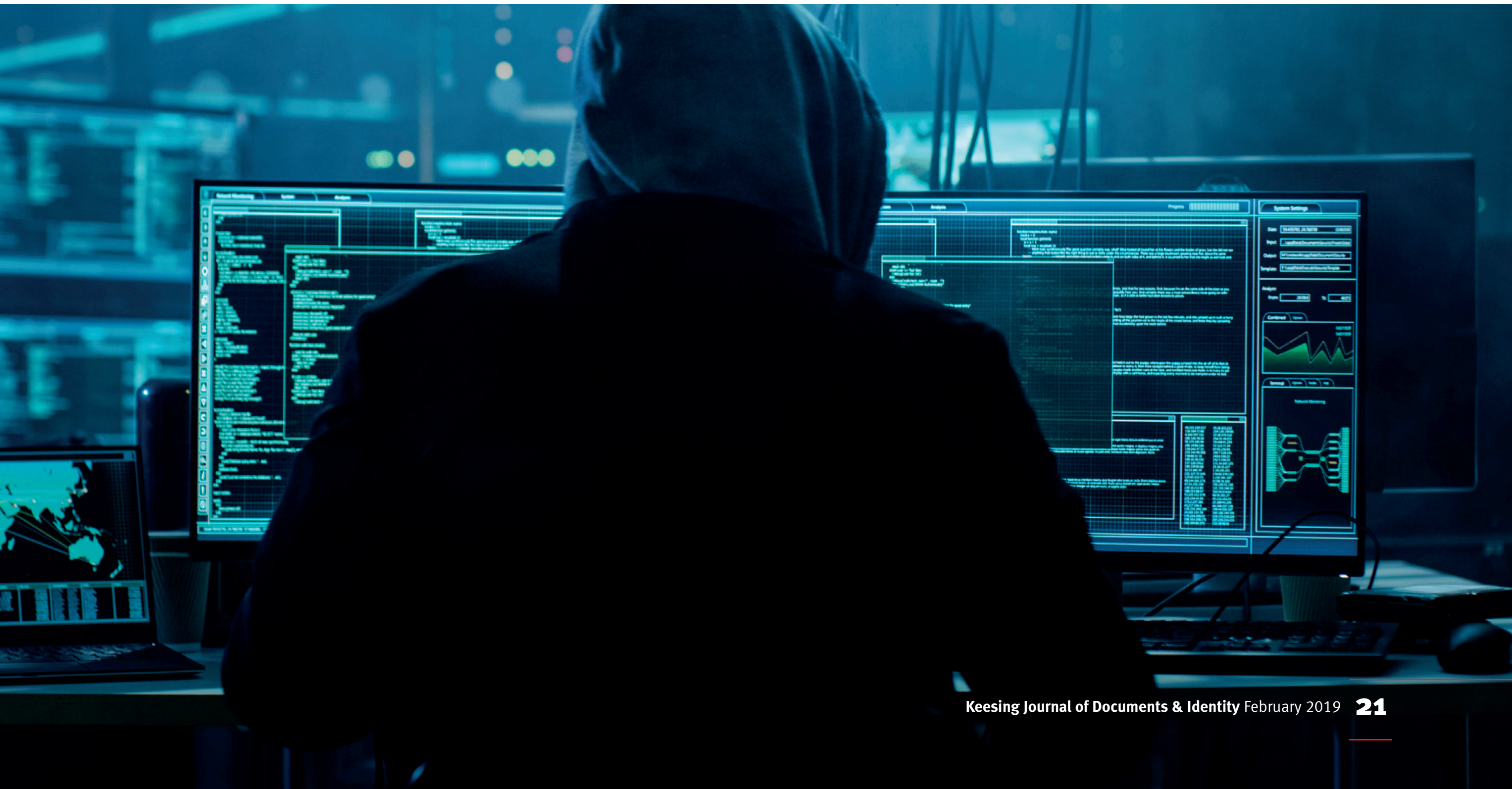
Some governments – such as the Dutch government – have successfully profiled individuals and their environments. However, there was no geo-localisation involved due to privacy laws. According to these, there is the ethical requirement that the services provided should benefit the individual, and that data may only be used for the purpose for which it was obtained. Ethical and legal constraints have been limiting governments in their use of predictive methods while commercial options seemed rather 'open-sky' in comparison. However, in the past few months there has been a paradigm shift.

A combined model: commercial methods in a public sector scenario

Because of this trend, the author is convinced governments could learn from the private sector where big data is used as a basis for targeted marketing strategies. It could be utilized to enhance models of criminal projections beyond the mere description of incidence patterns. How predictive analytics can improve crime prevention has therefore become the subject of a study. This study has resulted in two different approaches which could help prevent more crimes. The first communication-focused approach is relatively conservative, while the second geo-localisation-based approach is more exploratory.

Approach 1: Focus groups

In this scenario 'focus groups' are defined, based on anonymised profiling of individuals and their likeliness to be involved in crimes. This is similar to websites using anonymised data from users to improve their services as stated in their terms of use. Using this anonymised and clustered information, communication strategies can be developed which use specific digital channels to communicate with these individuals. After



further research psychological tools may be developed that allow police to prevent crime by attacking its causes before the crime occurs. This approach expands on the ProKid risk assessment tool used in the Netherlands and adopts research published in PLOS One by Michael Liebrenz suggesting the viability of such correlations.[3] There is further evidence of success in influencing human behaviour from the field of marketing. The ethical and legal constraints should be manageable as a specific use case has been defined. It serves the public interest and it is not overly invasive, as the privacy of the individuals involved is respected.

Approach 2: Motion patterns

The second approach expands on the first approach: generating personal profiles which are then matched with risk profiles. However, this approach involves capturing the motion patterns of the anonymous individuals which are then overlaid with 'near repeat' models. The expected benefit is that calculated hotspots will be enhanced with a crime probability indicator. The correlation between generic crime patterns and motion patterns of individuals with a computed crime potential could add value. From an ethical and privacy protection point of view, it is at this point in time not relevant who this person is, as the system does not focus on pre-emptive intervention. It just serves to establish more relevant hotspots.

An additional benefit is the ability to select the most appropriate intervention based on a suspected personal profile: What kind of intervention is appropriate and most effective? A similar consideration would be to prioritise intervention in suspected crime and choose a different approach if profiles are associated with various crime scenes rather than individual, localised crime. This approach relies on the cooperation between private and public entities. The police would make sure to acquire anonymous data from individuals matching predefined correlation models. Upon a hit, they receive this data tagged with the crime type and expected motion pattern in the next predefined time slot. The motion pattern could be as accurate as the pre-crime system, for example, 200 × 200 metres.

Discussion

The study has produced two models which show how marketing methods and big data-based profiling can enhance the conventional, case-focused crime prediction models. The first model focuses on focus groups whose consent have been obtained. The data is processed anonymously and the preventive measures have a broad focus. The second model builds on the first, but adds motion patterns and is overlaid with the existing pre-crime systems resulting in cause-enriched predictions. Both methodologies were the result of this study's findings and both aim to enhance problem-oriented policing, be it through different approaches.

The models seek to understand the underlying causes by incorporating findings from community policing as well as findings from big data analytics. The first model takes an educational approach, while the second adds context to the pre-crime analytics forecast, helping the police decide how to act on the prediction.

Increasing efficiency and accuracy

Both approaches aim to help the police make the most of their limited resources, mirroring the original reasons for the pilot project of the Kent Constabulary and considering the limitations of Buckley's study in 2014.[4] Especially the second model specifically implements the recommendations of Steinebach et al, to take demographics into account (such as age) as this may improve the prediction models and help identify appropriate measures.[5] Battersby's research into human and systemic interrelationships is especially relevant here, as it may help reduce the number of undiscovered and unpredictable actions and interactions.[6] The case study in Shreveport, Louisiana, described by Perry et al suggests this approach may be successful.[7]

Various referenced case studies from the field of marketing such as those involving SK Telecom, Alibaba and Netflix suggest the required technologies are already available. Especially credit card companies are already analysing the patterns of persons in order to detect unusual behaviour which may be a sign of fraud.

The general feasibility and legality of personal profiling has been discussed and confirmed by big data expert Bernhard Marr.[8][9][10][11][12] The German privacy law expert Thilo Weichert already confirmed that the private and public sectors are subject to different legal frameworks.[13][14][15][16][17][18] The specific way forward and the framework law for such programs need to be discussed on a national level and in context of the evolving EU data protection regulation. The Dutch police data scientist Dick Willems has suggested a step-by-step implementation, promoted as scientific research without investigative power.[19] This might give more legal leeway, and help increase support from politicians and society to adapt the legal framework.

The applicability of these findings and procedures are strongly dependent on a digital society. People who do not use the internet or leave very limited data trails can barely be profiled using this approach. However, for organised criminals and large criminal organisations communication is essential to their success. Therefore, the vast potential of big data as a crime prevention tool makes this prerequisite quite acceptable. Furthermore, this approach depends predominantly on the current and future developments in the data protection acts governing the public and private sector.

Window of opportunity

It must be acknowledged that the approach makes use of the current differences in the laws that apply to the public and private sector, which may only be temporary. The successful approach in the Netherlands makes use of both this window of opportunity and the combination of scientific work, limited population concerned and the positive effects for this population. During this window of opportunity further research needs to be done and additional proofs of concept need to be created. This will help convince politicians, legal entities and the public that the advances in pre-crime analytics are worthwhile and that their privacy is respected.

Ethical dilemma

A major issue in traditional modelling and correlating personal profiles with an increased likelihood for committing crime is the problem that – depending on the place and type of crime – over 80% of the cases remain unsolved. Some of these cases will never be connected with identified criminals. Other criminals may not have been caught. These individuals or groups seem to have developed a successful, covert modus operandi. The conventional detection models probably fail to identify the majority of criminals. This is especially important, as the number of false alerts has to be zero or extremely low for such a system to be ethically and legally acceptable. The ethical aspect is even more pronounced when it comes to repurposing and recombining information captured for a different use. The arguments that higher social values are served and the repurposing of the location data is kept to a minimum, may still be flawed. Governments are sourcing their data from the private sector where it was collected for commercial purposes. By using, supporting and obviously financing the operations there is a risk of an uncontrollable interdependence which could corrupt the control over privacy laws governing the private sector.

References

1 *Peterson, M. (2005). Intelligence-Led Policing: The New Intelligence Architecture.*

2 *Cheng, R. (2018). Seizing Data Overseas from Foreign Internet Companies under the CLOUD Act https://forbes.com/sites/roncheng/2018/05/29/seizing-data-overseas-from-foreign-internet-companies-under-the-cloud-act/#373925250c97 [Accessed 3 October 2018].*

3 *Gamma, A., Schleifer, R., Weinmann, W. and Buadze, A., L.M. (2016). Could Google Trends Be Used to Predict Methamphetamine-Related Crime? An Analysis of Search Volume Data in Switzerland, Germany, and Austria. U. S. Donald R. Olson, New York City Department of Health and Mental Hygiene ed.*

4 *Buckley, J. (2014). Managing Intelligence A Guide for Law Enforcement. CRC Press.*

5 *Steinebach, M., Halvani, O., Schäfer, M. and Winter, C. (2014). Begleitpapier Bürgerdialog - Chancen durch Big Data und die Frage des Privatspärenschutzes.*

6 *Battersby, P. (2014). The Unlawful Society – Global Crime and Security in a Complex World. Palgrave Macmillan, Basingstoke, New York.*

7 *Perry, W.L., Mcinnis, B., Price, C.C., Smith, S.C. and Hollywood, J.S. (2013). Predictive Policing – The Role of Crime Forecasting in Law Enforcement Operations. Rand Corporation.*

8 *Marr, B. (2010). COMPANY THE INTELLIGENT Five Steps to Success with Evidence-Based Management. Wiley Publishing, Inc.*

9 *Marr, B. (2015). Big data : using smart big data, analytics and metrics to make better decisions and improve performance. Wiley Publishing, Inc., Chichester.*

10 *Marr, B. (2015). Key Performance Indicators for Dummies. John Wiley & Sons, Ltd.*

11 *Marr, B. (2015). The 5 Biggest Risks of Big Data. https://web.archive.org/web/20180126100055/http://data-informed.com:80/the-5-biggest-risks-of-big-data.*

12 *Marr, B. and James, C. (2011). More with Less - Maximizing Value in the Public Sector. Palgrave Macmillan, Basingstoke, New York.*

13 *Weichert, T. (2005). Datenschutzrechtliche Anforderungen an Verbraucher-Kredit-Scoring. Datenschutz und Datensicherheit. DuD, 29 (10) (October), pp.582–587.*

14 *Weichert, T. (2012). Codex Digitalis Universalis, Datenschutz und Überwachung in ausgewählten Staaten. In: A. Schmidt & T. Weichert eds. Datenschutz. p.344pp, 418pp.*

15 *Weicher, T. (2013). Big Data und Datenschutz. Datenschutzakademie Schleswig-Holstein, Jahresprogramm 2013, pp. 1-22.*

16 *Weichert, T. (2016). Interview 25 October 2016.*

17 *Anderson, C., Baecker, D., Glaser, P., Hagner, M., Helbing, D., Latour, B., Schirrmacher, F., Weichert, T. and Weinberger, D. (2013). Big Data - Das neue Versprechen der Allwissenheit. unseld Son. H. Geiselberger & T. Moorstedt eds. Berlin, Suhrkamp.*

18 *Verlag für Polizeiwissenschaft (2012). Jahrbuch Öffentliche Sicherheit 2012/2013.*

19 *Willems, D. (2014). CAS: Crime Anticipation System – Predictive Policing in Amsterdam. https://www.slideshare.net/socialmediadna/crime-anticipation-system-cas-predictive-policing-in-amsterdam [Accessed 3 October 2018].*