Crime Prediction Technologies

Nadine Liv
Crime Prediction Technologies

The term “pre-crime” was coined in the film “Minority Report”, in which a criminal event that has not yet occurred is predicted, and a special police unit called “pre-crime” places the would-be offender in preventive detention in order to prevent him from carrying out the crime. The film deals with the legal and moral difficulty arising from a pre-crime methodology — arresting people who have not violated the law; this is a basic paradox because if the crime is prevented, then the prediction will turn out to be wrong.\textsuperscript{1} While predictions in the film are made in a fictional manner by three “prophets”, there are technologies today that are used to predict crime.\textsuperscript{2}

Increased Usage

The leading company in crime prediction technologies is PredPol (Predictive Policing). PredPol has a limited definition of crime prediction; namely, the practice of identifying dates and locations where specific crimes may occur and sending a patrol to these areas to prevent the occurrence of these crimes. The company proclaims that its goal is to help law enforcement agencies maintain safer communities by reducing the number of victims. The tools used by the system identify when and where crimes may occur, and allow the police to allocate resources effectively to prevent them from occurring. The information used by PredPol is very important and the company makes predictions based solely on data reported to the police. The information is anonymous, and the company does not collect Personally Identifiable Information (PII). The company proclaims that

\begin{itemize}
\item\textsuperscript{1} Minority Report (2002) directed by Steven Spielberg
\item\textsuperscript{2} Pre-Crime (2018) directed by Monika Hielscher & Matthias Heeder
\end{itemize}
protecting the privacy and civil rights of members of the community is as important to it as protecting the community from crime.\(^3\)

Another company, HunchLab, is a web-based proactive patrol management system. The company uses advanced statistical models that predict when and where crimes are likely to occur and the best ways for police to respond. According to the company website, policing tactics should not only be effective, they should reflect the community’s priorities. Therefore, the company provides features that align patrol activities with the community’s priorities, allocate resources to prevent over-policing, and determine which tactics work and which ones do not.\(^4\)

There are two approaches to crime prediction. One examines geographic information in order to identify “hotspots” where a crime is likely to occur in the future, thus enabling police units to increase surveillance in these areas. The second analyzes social networks and behaviors in order to identify potential criminals or, alternatively, those at increased risk of victimization.

Such technologies are increasingly being used worldwide. One example is the Chicago, IL, Police, which teamed up with a professor at the Illinois Institute of Technology to develop an algorithm called the “Strategic Subject List” (SSL) to assess and examine individuals at a high risk of being involved in a violent event. The algorithm calculates a risk assessment and the likelihood that a person will be involved in a violent crime incident — either as a criminal or as a victim — and ranks people on a scale ranging from 0 (low risk) to 500 (high risk).\(^5\) For prediction purposes, the system uses many databases, including surveillance cameras and social media.\(^6\)

Another example is the Fresno, CA, Police, which works with the ‘Beware’ system. The system has access to databases of banks, courts, and any institution that deals in money lending. The software can access all these databases at the same time. When a call arrives at the emergency call center, it is classified as a life-threatening situation or a crime in progress, and an address is attached to the call. The ‘Beware’ system automatically searches all these databases and provides the recipient of

\(^3\) [https://www.prepdol.com](https://www.prepdol.com)  
\(^4\) [https://www.hunchlab.com](https://www.hunchlab.com)  
\(^5\) [https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np](https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np)  
\(^6\) Pre-Crime (2018) directed by Monika Hielscher & Matthias Heeder
the call with real-time, precise information about the address that includes the names of the people who lived there in the past, who live there currently, their cell phone numbers, previous addresses and associates; the system also searches social media and gathers information that might indicate a threat. The Fresno police chief explains that *if the algorithm used by the private sector is successful in segmenting the target audience for sales, it is worth exploiting the advantage provided by the algorithm to improve law enforcement* in preventing crime.\(^7\)

The London Police uses a technology system called ‘Matrix’, which is similar to its counterpart in Chicago. It identifies people, connects them, *investigates patterns in social networks*, calculates statistical probability, ranks people and provides alerts.\(^8\)

*Therefore, there are two approaches to crime prediction. One examines geographic information in order to identify “hotspots” where a crime is likely to occur in the future, thus enabling police units to increase surveillance in these areas. The second analyzes social networks and behaviors in order to identify potential criminals or, alternatively, those at increased risk of victimization.*\(^9\)

**Terrorism Prevention**

Since terrorism is a special case of crime, crime prediction may also be used to predict and prevent terrorism. At the end of February 2018, the Israel Police and the cyber labs of Ben-Gurion University of the Negev established a joint research center for computational criminology. The center, which was launched at the National Cyber Campus in Beer Sheva, is involved in the development of cyber enforcement and prevention by developing dedicated tools based on advanced research tools in the field of big data. In the new center, Israel Police officers are collaborating with university researchers with a worldwide reputation in the field. According to Prof. Lior Rokach, chair of the Department of Software and Information System Engineering at the university and director of the center, this is a breakthrough in the field of cyber and artificial intelligence that serves as a significant milestone for enforcement authorities, comparable to the discovery of the DNA sample.\(^10\)

---

\(^7\) Pre-Crime (2018) directed by Monika Hielscher & Matthias Heeder

\(^8\) Pre-Crime (2018) directed by Monika Hielscher & Matthias Heeder


\(^10\) [http://in.bgu.ac.il/pages/news/Computational-Criminology.aspx](http://in.bgu.ac.il/pages/news/Computational-Criminology.aspx)
Criticism

Crime prediction is one of the most controversial topics in the field of criminal justice today. Studies maintain that this statistical based, analytical approach works; however, crime prediction may open a Pandora’s box of problems.¹¹

Most predictive models are information-based rather than theory-based, which may have implications for the way in which these models are used. The use of big data-based approaches may result in a great deal of emphasis on correlation rather than causality.¹² The police’s handling of potential suspects must be done on the basis of individual suspicion and not on the basis of statistical probability;¹³ as happened in the case of Robert McDaniel. One day, McDaniel was paid a home visit from a Chicago Police officer informing him that a police algorithm had produced a list of 400 suspects with the potential to be involved in a violent incident (as criminals/victims) and that he was rated 215 out of 500. McDaniel was placed under surveillance and warned to avoid committing crimes lest he bear the consequences and be judged with the full severity of the law. The rating was given to him on the basis of a variety of characteristics, including a list of associates involved in violent incidents, his neighborhood and the existence of prior criminal cases relating to personal drug use offenses. McDaniel himself has no history of violence.¹⁴

The main problem hovering over the issue of using crime prediction technologies is the relationship between the private sector and law enforcement agencies. There is a concern for privacy protection when Internet users are willing to disclose their personal information to companies in the private sector, such as Google and Apple, but are generally less willing to volunteer information to the government. In the current situation, we see technology companies gathering information and then selling it or offering it through various services to the police. Even if the information is not in the hands of the police, it is in the hands of private companies; the technology collects as much information about us as possible.¹⁵ In addition, the technology provided by the prediction companies is patent-protected and lacks transparency. Therefore, law enforcement agents cannot fully understand the results produced by the software and they rely on it blindly. This creates a

¹¹ https://www.floridatechonline.com/blog/criminal-justice/4-problems-with-predictive-policing/
¹⁵ Pre-Crime (2018) directed by Monika Hielscher & Matthias Heeder
problem of accountability and begs the question: Who is responsible for exercising the discretion of the law enforcement system: law enforcement agencies or technology companies?16

Rating for the purpose of risk assessment, as used by the Chicago Police, may create negative criminological labeling, reeling an innocent person into a life of delinquency and crime. Therefore, between the two approaches to crime prediction, it is recommended to stick to the narrow approach, which only analyzes geographic information while avoiding behavioral analysis on social networks.

Another result of the lack of transparency is the strengthening of a racist bias. Using a crime prediction model for “profiling” may result in stigmatization among individuals and groups, and create discrimination based on algorithms. Decades of criminological research show that crime reports are based on statistics collected by the police and document the police response to crime rather than provide full reports of actual crime. Automatic prediction based on biased - though seemingly neutral — information from the outset actually reinforces cognitive biases.17

Summary

In criminology, labeling theory holds that society responds to every act by an individual by attaching a positive or negative label to the act. The individual then internalizes the positive or negative label he has been assigned and acts accordingly as “a self-fulfilling prophecy”.18 Thus, if a person receives a positive label, he will internalize the positive label and behave normatively in society. If he receives a negative label, he will internalize negative label and behave in a way that deviates from the accepted rules of the given society.

Rating for the purpose of risk assessment, as used by the Chicago Police, may create negative criminological labeling, reeling an innocent person into a life of delinquency and crime. Therefore, between the two approaches to crime prediction, it is recommended to stick to the narrow approach, which only analyzes geographic information while avoiding behavioral analysis on social networks.

---

18 לפקס, משה. השפעת התוויות ספרות התרבותית-وغיימית. דר_matteo.pdf

ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations.