Cyber Profiling in Criminal Investigation

3

Szde Yu
Wichita State University, USA

INTRODUCTION

As technologies are progressively ingrained in modern life, the line between street crimes and cybercrimes has become gradually blurry. Nowadays, in almost all criminal investigations there is a need for digital investigation to be incorporated as digital information has become relevant and even crucial in most cases. Investigators often have to rely on information retrieved from electronic platforms to find leads and evidence even in crimes that would be traditionally considered street crimes. When comprehensive information is not always attainable, the use of cyber profiling may provide further insight into crucial questions regarding identity, time, and location. Cyber profiling is an analysis on the digital footprints associated with a person whose identity may or may not have been known. When the identity is unknown, the purpose of cyber profiling is primarily about identifying this person or at least creating a workable profile that narrows down suspects. When the identity is already known, the purpose is usually aimed to reveal information that is not readily visible, such as personality, motives, or linkage to other crimes. Besides being subject-centered, cyber profiling can also be event-centered in an attempt to identify time and location. As such, cyber profiling has a wide variety of application in criminal investigation and yet it has not been duly valued. This chapter introduces the fundamentals of cyber profiling and calls for more attention to the development of this technique.

BACKGROUND

To date, there is very little research effort in developing or validating cyber profiling. Therefore, it could be easy to dismiss cyber profiling. Yet, cyber profiling actually has been widely applied in many fields, albeit the name might not be recognized. In other words, many people are already experiencing cyber profiling without knowing it. For instance, some experts tend to make diagnosis about a public figure's personality or state of mind based on comments made on Twitter or other social media. This is basically a form of cyber profiling as the inference is based on digital footprints in the absence of any physical contact. When people do online shopping on certain products and consequently receive promotional advertisements about similar products, it is another example of cyber profiling because the online vendors are profiling shoppers based on their past shopping habits so as to decide what other products they would be interested in as well. Online dating services like Tinder also allows users to do cyber profiling based on only a few photos before they decide which stranger they want to go out on a date with. If cyber profiling can be relied on in the business world and social media, there is no reason why it cannot be utilized in criminal investigations.

DOI: 10.4018/978-1-7998-3479-3.ch024

Currently, criminal investigators are already used to looking for clues in a subject's digital footprints, such as text messages, emails, social media postings, and online shopping or browsing records (Rogers, 2003). However, cyber profiling calls for more attention to the implicit information hidden in the digital footprints. For instance, a man might intentionally avoid expressing his political view on the Internet, but from an analysis on the videos he watched on YouTube and the news websites he frequently visited we can still deduce what this man's political stance is, provided access to such digital footprints is not an issue. The same analysis might shed light on other aspects as well. A study was conducted on Facebook to test the reliability of cyber profiling (Yu, 2013), and it found that using nothing but the participant's Facebook public information, it is possible for a trained profiler to draw largely accurate conclusions about the participant's race, age, gender, and nationality. Moreover, profilers may correctly infer a person's certain personality traits, such as self-control based solely on digital footprints. Lambiotte and Kosinski (2014) also reported the ability to predict personality based on publicly available digital footprints, and they believed such prediction will become more and more accurate as more electronic data are being generated on a daily basis. This type of prediction, aka cyber profiling, can apply to criminal investigation and become a huge help.

Being able to predict personality and characteristics like gender and age has always been an important aspect of criminal profiling (Williams, Nathanson, & Paulhus, 2010; Douglas & Burgess, 1986; Piniz-zotto & Finkel, 1990; Canter, 2004). While traditional criminal profiling focuses on behavioral evidence (Turvey, 2011), it becomes crippled when there is no physical trace serving as behavioral evidence. It is a serious issue in modern day investigations where many social interactions only take place in the virtual world (Rogers, 2003). In this regard, cyber profiling uses digital footprints as online behavioral evidence to look for information that can identify characteristics and personality (Yu, 2013). If identifying information can be directly retrieved, then profiling is not needed. For example, it should be easy to tell a person's gender and race by simply looking at the person's selfies. Profiling, however, becomes crucial when such identifying information is vague or deliberately disguised. For instance, when a 46-year-old man pretends to be a 16-year-old girl on the Internet, the photos shared by him probably should not be trusted. In an era where almost everyone has some sort of online presence, it is imperative for criminal investigators to possess the skills and knowledge to verify the authenticity of each online persona they encounter in the course of investigation. This is where cyber profiling begins. Further, from the online persona's digital footprints, investigators should develop skills to find useful clues and evidence that can point to the right person and the right place. Moreover, investigators ought to be able to recognize potential linkage among the digital footprints generated by different online personas in case they are actually owned by the same person. For example, a person can own multiple accounts on Facebook or Twitter and use each account to play a different role in cyberspace. Can the investigators see through this and make connections? This is where cyber profiling helps.

Unfortunately, cyber profiling is not yet a technique that law enforcement agencies are concerned with, even though their agents constantly have to look for clues in a suspect's or a victim's digital footprints. Most of the time, investigators only see what is there to be seen, and tend to overlook what is hidden or implicit in the digital footprints. For example, some researchers found that criminals could easily disguise incriminating communication as email spam and investigators would likely overlook it even when the disguise is very primitive (Yu, 2015). In this regard, cyber profiling may help reveal what is not so obvious to be seen considering incriminating information is usually implicit.