Andrew g. ferguson's overview on dig data policing

At the “ high-tech command center” located in Los Angles, computers manage live crisis, maps pin point high crime areas, and surveillance cameras monitor streets. This center is the Real-Time Analysis Critical Response Division (RACR) (Ferguson, 2017, p. 1). It provides law enforcement with intelligence and information in a matter of minutes after a crime as occurred. Technology such as this is changing the way the world works. From medical miracles to infrastructure developments and law enforcement. These advances in technology are reconfiguring the norms and relationships in domestic policing throughout the United States. Predictive policing has proven to be an important advantage to law enforcement- if carried out correctly. A professor, scholar, and expert in privacy, predictive policing, and the Fourth Amendment, Andrew G. Ferguson provides a comprehensive overview of policy and potential harm of big data policing (Ferguson, 2010).

Throughout the book, Ferguson analyzes big data policing and how it can alter the way police departments operate. Ironically, predictive policing was designed to prevent social injustices and discrimination across the agencies. Ferguson’s comprehensive overview in *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* covers both the capacities and the potential risks associated with predictive policing. This well-written narrative uses documented studies and a deep knowledge of predictive policing to examine the bias and errors associated with the data used. He warns that flawed data can lead to “ aggressive police presence, surveillance, and perceived harassment,” particularly in “ poor communities of color” (Ferguson, 2017, pg. 3). While these new advances in technology

open a window of opportunity for the law enforcement community, this environment also comes with several dangers. By exposing the issues and providing an explanation of data-driven policing, Ferguson hopes that society can plan for a future of big data.

The chapters of the book are divided into three sections. Chapters one and two explain what big data policing is, and the technology reform in domestic policing. Ferguson discusses how data is not collected solely from law enforcement, but from a “ web of interrelated, interconnected groups” (Ferguson, 2017, p. 7). These chapters also describe legislative acts designed to protect consumer privacy and how “ these laws do not prevent law enforcement access” (Ferguson, 2017, p. 17). Chapter three through six provide an overview and examples of how big data policing is implemented. Each one represents a different domain of big data’s effect on policing practices. It explores the who, where, when and how of predictive policing. Ferguson warns of the discriminatory nature in policing as well as information about the transparency of using big data. In cities like Chicago and New Orleans, individuals most likely to become victims or perpetrators of violent crimes are compiled and maintained on a “ heat list.” It focuses on eleven variables to determine what risk an individual is at. Those variables include narcotic offenses, violent crimes, and weapon offenses. Individuals identified by the algorithm are rarely, if ever provided with the information as to why and how they became listed. Chapter five, “ When We Police,” rightfully cautions that reliance on automated systems causes a wider margin of error. There is no way to check the accuracy of information, thus the use of common sense becomes less common (Ferguson, 2017, p. 97).

Chapter six sets the stage for chapter seven in that it focuses on how the turn from small data to big data can have adverse effects on the civil liberties for members of minority groups. Ferguson mentions the disparity of data related to the people and communities of color. In chapter seven, he coins the term “ Black Data”. During this section Ferguson explains the problematic nature of big data policing. The predictive models discussed in the early chapters of the book “ falsely flag black defendants at almost twice the rate of white defendants” (Seigel, 2019). Although promising a “ clean start,” even big data policing cannot escape racial discrimination (Ferguson, 2017, p. 133). Arguably, “ black data” is the cornerstone of the entire book. It focuses not only on racial bias, but transparency and constitutional law.

Beyond that of race, Ferguson discusses how big data policing lacks transparency and impedes upon Fourth Amendment rights. He compares these data systems with “ black-box mysteries” and explains just how complex these algorithms are (Ferguson, 2017, p. 136). Despite admitting that the data systems lack transparency, Ferguson falls short of demanding it. Instead, he calls more so for accountability. The inner workings of the algorithms that run our lives are far too complicated for the average person to comprehend. The issue of transparency leans more towards why these algorithms are being implemented and less towards how the mathematical equation works. The hysteria that “ big brother” is always watching is not transparency of the algorithm itself, but of how that algorithm is put into use. Ferguson provides an excellent explanation of the differences between accountability and transparency. Having accountability for the system and data used will require big data policing to “ confront the problems raised in

this book” (Ferguson, 2017, p. 139). The last portion of chapter seven explains the constitutional issues surrounding big data policing. Ferguson singles out the Fourth Amendments doctrine. In an interview by ‘ The Crime Report’, Ferguson speaks on this topic in his book. Big data can skew reasonable suspicion. The fact that someone is ranked on Chicago’s “ heat list” does not justify reasonable suspicion. The technologies used in predictive policing prove to be problematic in restricting suspects of their Fourth Amendment rights. The Supreme Court Case *Carpenter vs. the United States* (2018) is used by Ferguson as an example to discuss third-party record acquisition. Although the court held that the acquisition of these records violated the Fourth Amendment’s right against unreasonable search and seizure, Ferguson continues explaining how uncertain our expectation of privacy is. “ What we share with others, we don’t necessarily think we are sharing with the police” (Pagnamenta et al, 2018).

The last few chapters, Ferguson shifts focus to discuss the more positive aspects of big data policing. Just as algorithms flag suspected criminals, they also flag police abuses. He coins the additional terms “ blue data” and “ bright data”. As aforementioned, “ blue data” is the ability to predict police abuse and techniques. Agreeably, the lack of such blue data is unacceptable. There is no police database to track bias among officers. At least not yet. Chapter 8 connects the relationship between police reform and big data surveillance. A refreshing turn of events comes with the onset of “ bright data.” Instead of pointing out flaws associated with big data policing “ bright data” focuses on remedies to correct problems. Big data surveillance identifies an issue, but it does not provide a solution. Ferguson outlines

alternative remedies for solving and reducing crime that does not require police involvement. “ In thinking of predictive policing as only a policing tool, the community may fail to see other solutions to the identified environmental risks” (Ferguson, 2017, p. 169). Overall, the reasons for high crime stems from a variety of underlying factors. Responding to and attempting to correct those with police involvement fails to improve the situations. At best, it provides a temporary fix. Ferguson’s observation and study provides insight to a never-ending quest.

The Rise of Big Data Policing is a tremendously well-versed and inclusive review of the current stance of big data policing. Ferguson’s expertise and strong research make it a ‘ must read’ for anyone interested in surveillance techniques and the potential threats big data imposes on citizens. Not only does this work provide a comprehensive overview of the risks and potential dangers of big data policing, but it also provides a thorough explanation of how big data can be beneficial in fighting issues of racism and bias. Technologies used for big data policing all share a common factor. It identifies risk factors that can contribute to criminal activity (Ferguson, 2017, p. 167). *The Rise of Big Data Policing* is informative, easy to follow, and provides a unique insight to the effects and techniques associated with big data.

- Ferguson, Andrew G. (2010). Andrew Guthrie Ferguson Professor of Law. Retrieved May 29, 2019, from https://www. law. udc. edu/page/AFerguson

- Ferguson, A. G. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York, NY: New York University Press.
- Pagnamenta, J., Ponte, Y., Cipriano, A., McDermott, M. M., TCR Staff, & Justice News. (2018, May 03). The Perils of Big Data Policing. Retrieved from https://thecrimereport. org/2017/12/20/the-perils-of-big-data-policing/
- Siegel, E. (2019, January 30). Predictive policing: Data can be used to prevent crime, but is that data racially tinged? Retrieved from https://bigthink. com/big-think-books/is-crime-prevention-data-racially-biased