Book Review: Ferguson, Andrew G., *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement.* **New York University Press, 2017. ISBN: 9781479892822 (Hardcover). 272 pages. $28.00.**

Reviewed by Robert L. Smith[1]

In *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement,* Andrew G. Ferguson, addresses how 'high tech' data collection, surveillance technology, and predictive targeting are utilized and applied in modern police practices and how minorities and poor communities are policed and affected. Throughout the book, the author discusses how these same technologies can be used to identify police misconduct and improve effectiveness and accountability within law enforcement agencies. And, he suggests these technologies could potentially be used to identify underlying influences for high risk factors, such as, socioeconomic perils, environmental risks, education, and job training deficiencies and ameliorate these with social service resources rather than merely focus on crime control.

Professor Ferguson has taught law at the David A. Clark School of Law in the District of Columbia since 2010 and is a Senior Visiting Fellow at the Harvard Law School's Criminal Justice Policy Program and a Policing Data Fellow at the NYU Law School's Policing Project. The author was also a Law Clerk in the US 5th Circuit Court of Appeals in 2000. He also worked for the Georgetown Criminal Justice Center in Washington DC and the Public Defender Service for the District of Columbia as a Supervising Attorney from 2001 to 2010. Given his academic and professional experience, the author is considered an expert on predictive policing, big data surveillance, and the Fourth Amendment.

---

[1] **Robert L. Smith** has an M.S. in Criminal Justice from Lamar University in Beaumont, Texas and has been a commissioned Texas peace officer for over twenty-seven years. Address correspondence to: Robert L. Smith, e-mail: rsmith4@lamar.edu.

The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement offers a very complete assessment on the use of "big data" by law enforcement and discusses real time camera monitoring in public spaces, facial recognition, and biometric data bases. The book also delves into data mining and describes how sophisticated technologies are capable of amassing a trove of personal information, consumer transactions, and personal communications collected and stored in law enforcement data bases merged with crime data, warrant information, and other police intelligence in order to "revolutionize policing" with predictive policing and intelligence driven strategies.

In his book, Ferguson is very methodical and the first chapters define the "rise of big data" and explain what is collected, the methods and sources of collecting data, and how the data is obtained, categorized, analyzed and used by law enforcement to develop policies and practices that target, map, and identify criminal suspects. The author also discusses how technologies are used to identify locations that are potentially 'high crime environments,' as well as persons that may be at-risk of being victims of crime. The information gleaned from the data can be used for preemptive, preventative, and proactive police action.

According to Ferguson, although a "complete big data convergence" between private entities and "public" collection of data by law enforcement has not "yet occurred," (26) he cautions that information collected for consumer tracking purposes, as well as information voluntarily provided by users and consumers on social media, and to private third parties, reduces individual privacy. The concept of notice and choice is described: If companies provide privacy practices notice, and people have a choice to provide data or not, the privacy is 'sufficiently protected' (Martin 2016). However, without a viable "opt out," the data may be collected and shared, sold, or subject to legal process. To make matters worse, data brokers, collect personal information from various sources including publicly available sources, government records, financial information, and census data. These actors sell the information to many parties, including law enforcement. Credit bureaus maintain financial information, and other companies use purchase habits and history for marketing. As Martin (2016) notes, the data can also be used by these companies for fraud prevention and determining credit worthiness and risk assessment.

In his book, the author discusses private company partnerships with the government that develop software and platforms to track terrorists and criminals which can reveal and connect information to build clues that were previously hidden in data sources used by law enforcement in

the past. He writes, the monitoring of public social network environments, such as, *Facebook* and *Twitter* can be used to populate government databases, fusion centers, or information repositories that provide and share information with government and law enforcement organizations. Health, education, crime records, surveillance cameras, photographs, fingerprint and DNA databases, such as, CODIS (developed to collect DNA samples from those sentenced and confined in prisons to compare with unidentified DNA samples collected at crime scenes with unknown suspects) are used to identify patterns which may lead to detecting criminal activity, or even what may appear as evidence of preparation to commit criminal acts, such as, suspicious transactions, travel patterns, supplies, tools, and material purchases consistent with items commonly used in some criminal behaviors.

Ferguson contends throughout his book that law enforcement organizations have experimented with data driven approaches in policing. The author cites New York City as an example, and the introduction of Comp Stat in the 1990s, as the beginning of data-driven methods that unfairly targeted poor communities and racial minorities. Comp Stat required police precinct commanders to report crime statistics weekly, and the data gauged benchmarks to address crime response and arrest rates in the precincts. Accountability for crime reduction was based on the statistics collected and was adopted as one of the first data driven systems by police management. (38). Police administrators in the Big Apple sought out "partnerships between police organizations, academic researchers, private sector businesses, and relied on federal grant money to study and implement 'big data' systems in law enforcement" and to study patterns of crime. (40) This "convergence," according to the text, established the tone for tension between police reform and "technocratic" pursuits. It is likely that this tension was mainly due to flaws in the programing architecture of software and computer databases used in "big data policing." Ferguson states big data applications uncovered wider established patterns in policing, based on systemic racism that was ingrained in historical police practices.

In his book, the author also illustrates how big data policing is currently employed. He discusses "person-based predictive modeling" which refers to the use of demographic information and affiliations and relationships in social, family, and other affiliations, such as, gangs or groups. High-risk individuals are identified for intervention or increased police attention. Ferguson offers the Chicago Strategic Subject List or "Heat List" as an example of how data is used to predict one's likelihood of either committing a crime or being a crime victim. As Ferguson

contends, in 2016, 80% of the 51 people shot over the Mother's Day Weekend had been identified on the 'heat list." On Memorial Day of the same year, 78% of the 64 people shot were also on the list. Regardless, of the impressive accuracy rates, due to an increase in shootings in the city, the model has been publicly criticized. Fears of racial bias, data errors, and a disregard for constitutional protections are cited by the author as serious challenges to a person based predictive strategy. Shootings are common in poor neighborhoods, and young black males are frequently crime victims and are more likely to be arrested. Therefore, if the data used in computer systems is based on human judgment, and is biased beforehand, some critics argue that the model simply cannot be trusted—at least not in the absence of independent oversight or audit of the data. Ferguson notes, however, that the same model is currently used in New Orleans by the city's fire department, public works agency, health department, as well as the police, to identify missing streetlights, street clean up, and liquor store violations. All "localized interventions" are from the same data set that mapped crime. (50)

The author also discusses "place-based predictive policing" systems which use crime data to make risk predictions about specific places and times. Ferguson argues the systems implement discriminatory biases inherent in policing practices and unfairly and disproportionately target racial and ethnic minority populations. The author contends that this may occur even if race or other protected classes are excluded from the algorithms. He contends that there is an artificially inflated nature of discrimination, when social affiliations, demographic information, and geographic location of "small data" and information from traditional policing models are used to inform big data analyses.

Ferguson's book demonstrates how police administrators use big data to predict crime. While the technology is new, police administrators have long sought to predict crime, and this is evident by the "beat" mapping, resource allocation, shift configuration decisions, seasonal increases, events, and other "timing" considerations which best suit the needs of the agency mission. Some beat cops are adamant that on payday Friday, especially the ones that fall on the beginning of a month, when government checks are issued, crime will increase. Some officers will even say that a full moon that coincides with payday weekends further exacerbates crime statistics. And, foot patrol officers know that summer months bring out more delinquent behaviors due to warmer weather and school holidays. Seasonal related tourism attracts criminals to unsuspecting strangers in areas normally free of significant criminal

activity. And, holidays usually have an uptick in family violence and child custody issues. These are only a few examples which illustrate that police have always been in the business of trying to predict crime—before it occurs.

In his book, Ferguson also examines real-time surveillance and investigation and how "big data" policing pieces together several otherwise dissimilar technologies for immediate information access and large-scale tracking. Police have historically gathered personal information; however, searchable comprehensive databases make the information available much faster. Ferguson also discusses how facial recognition developments, automatic license-plate readers, surveillance with drones and public space cameras, and localized and shared crime databases are used in investigations. He warns readers that these technologies are neither foolproof nor guaranteed to be accurate, and the margin of error is widened by human discretion. Information may also be recorded incorrectly and police may be likely to simply accept and act on the information at hand. Ferguson asserts the jump from "small" data to "big" data may undermine an individual's constitutional protections from police abuses and also raises civil rights challenges for members of racial and minority groups that have historically suffered from police abuse. In what he describes as "Black Data," Ferguson argues the problem with big data policing, as currently implemented, is that it leads to racially biased policing and undermines Constitutional liberties.

In an interesting twist, Ferguson also devotes a chapter of his book to "Blue Data," which is the inverted use of big data to predict police abuse. Ferguson suggests the same principles used to surveil and monitor citizens can be used to monitor police officers. Ferguson discusses how GPS tracking devices and body cameras can be used to track police officers in the field during the course of their eight-hour shifts. He argues that the use of algorithms can also be utilized to flag at-risk officers for complaints and improper conduct. While Ferguson claims field officers and police unions will likely push back against these new mechanisms of oversight, at least one recent research study indicates police officers may not be opposed to these practices (Gaub et al 2016).

Ferguson concludes his book with a call for transparency and input from citizens and stake holders in what he terms "surveillance summits." He argues that these informative meetings should be used to explain tactics as well as how data-driven technologies are employed. The author argues that big data police strategies can (and should) be audited and evaluated by members of the community. He argues that unbiased data, coupled with citizen "buy in," may lead to a safer, more humane society.

It is evident that Ferguson put a considerable amount of time and energy into this book. It is well-researched and is likely to be of interest to both the academic, as well as the criminal justice practitioner. It would make excellent supplemental material for virtually any graduate level course and is likely to generate important discussions. I recommend this book.

REFERENCES

Gaub, J. E., Choate, D. E., Todak, N., Katz, C. M., & White, M. D. 2016. "Officer Perceptions of Body-Worn Cameras Before and After Deployment." *Police Quarterly*, 19(3), 275–302. https://doi.org/10.1177/1098611116653398

Martin, K. 2016. "Data Aggregators, Consumer Data, and Responsibility Online: Who is Tracking Consumers Online and Should They Stop?" *Information Society*, 32(1), 51–63. https://doi.org/10.1080/01972243.2015.1107166