Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2016-09

Your criminal FICO score

Tonelli, Michelle

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/50496

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

YOUR CRIMINAL FICO SCORE

by

Michelle Tonelli

September 2016

Thesis Advisor: Rodrigo Nieto-Gomez
Co-Advisor: John Rollins

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE YOUR CRIMINAL FICO SCORE			**5. FUNDING NUMBERS**
6. AUTHOR(S) Michelle Tonelli			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

One of the more contentious uses of big data analytics in homeland security is predictive policing, which harnesses big data to allocate police resources, decrease crime, and increase public safety. While predictive analytics has long been in use to forecast human behavior, the framework has not proved to be a flawless undertaking. In an effort to improve outcomes of predictive policing, this thesis assesses two high-profile programs—the nation's most popular credit-scoring system and a federal flight-risk program—to determine the greatest pitfalls inherent to programs using predictive analytics. The programs are assessed using what is commonly known in big data as the four Vs—volume, velocity, variety, veracity—but with an added component of the author's creation: verification. Through this framework, it became apparent that the hardest Vs for any predictive policing program to fulfill are veracity and verification. As the field of predictive policing expands, programs face the challenge of ensuring that data used for analysis is accurate and remains accurate, and that the metrics used to verify risk assessments are sound.

14. SUBJECT TERMS predictive policing, predictive analytics, FICO, Secure Flight, Five Vs, risk assessments, big data			**15. NUMBER OF PAGES** 79
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

YOUR CRIMINAL FICO SCORE

Michelle Tonelli
Attorney-Advisor, Office of General Counsel, Department of Homeland Security
B.A., University of the South, 2005
J.D., New York Law School, 2009

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2016**

Approved by: Rodrigo Nieto-Gomez
Thesis Advisor

John Rollins
Co-Advisor

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

One of the more contentious uses of big data analytics in homeland security is predictive policing, which harnesses big data to allocate police resources, decrease crime, and increase public safety. While predictive analytics has long been in use to forecast human behavior, the framework has not proved to be a flawless undertaking. In an effort to improve outcomes of predictive policing, this thesis assesses two high-profile programs—the nation's most popular credit-scoring system and a federal flight-risk program—to determine the greatest pitfalls inherent to programs using predictive analytics. The programs are assessed using what is commonly known in big data as the four Vs—volume, velocity, variety, veracity—but with an added component of the author's creation: verification. Through this framework, it became apparent that the hardest Vs for any predictive policing program to fulfill are veracity and verification. As the field of predictive policing expands, programs face the challenge of ensuring that data used for analysis is accurate and remains accurate, and that the metrics used to verify risk assessments are sound.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

CAPPS	Computer-Assisted Passenger Prescreening System
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
FCRA	The Fair Credit Reporting Act
FICO	Fair Isaac Company
OMB	Office of Management and Budget
PNR	passenger name records
SORN	System of Records Notice
TSA	Transportation Security Administration
TSDB	Terrorist Screening Database

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

To use big data analytics effectively in predictive policing, a program must meet what has become known as the "four Vs"—volume, velocity, variety, and veracity.[1] Volume requires a large amount of data, velocity requires that the data be added and processed at high speeds, and variety requires that the data come from multiple sources. Some scholars argue that big data must also be accurate, which has become known as the fourth V—veracity.[2] Veracity is especially important when one is attempting to predict how a particular person will act. Because of the high stakes involved with predictive policing, the author argues that programs need to apply a fifth V—verification. Verification requires that the predictions from the predictive program be verified as accurate. It is the metrics to measure how well the program works. By using the Five V's as a framework, any predictive analytics system can be analyzed for accuracy and viability.

This thesis uses the Five V framework to review the FICO score and Secure Flight programs in order to determine what, if any, shortfalls exist. Through this analysis, it became clear that all predictive analytics programs have difficulty fulfilling all five Vs. FICO is able to fulfill volume because it keeps records for every individual who has some form of credit, which allows FICO a strong baseline. However, Secure Flight has a weak baseline because it does not have the proper volume of data. FICO and Secure Flight both have difficulties with velocity because each program must rely on third- or fourth-party data providers to update their records. FICO and Secure Flight also do not fulfill variety because each one draws only on one type of data. FICO mostly draws on financial data and Secure Flight draws on data from the government. This lack of variety can

[1] Janet Chan and Lyria Bennett Moses, "Is Big Data Challenging Criminology?," *Theoretical Criminology* 20 (2016): 21–39.

[2] Richard Berk and Justin Bleich, "Statistical Procedures for Forecasting Criminal Behavior: A Criminal Assessment," *Criminology & Public Policy* 12, (2013): 513–544, as quoted in Chan and Moses, "Is Big Data Challenging Criminology?," 28 *Theoretical Criminology* 20 (2016): 21–39, stating that accuracy is important for big data analytics; for further discussion, see "The Four Vs of Big Data," IBM Big Data & Analytics Hub, accessed Aug. 12, 2016, http://www.ibmbigdatahub.com/infographic/four-vs-big-data.

undermine the predictive quality of the risk analysis once score creep—or the use of the risk analysis for more than its original purpose—begins. Both FICO and Secure Flight already have seen score creep, and it is clear that score creep is a phenomenon that all predictive analytics programs must anticipate.

Finally, the author reviewed the programs using the two Vs that are the hardest to fulfill—veracity and verification. Even harnessing data that is fully transparent, FICO still has difficulty maintaining accurate records. Secure Flight also is unable to maintain fully accurate data. For both systems, one of the main problems with the veracity of the data is the ineffective redress programs that both rely on to fix inaccurate data. In addition, Secure Flight does not have reliable metrics because it is difficult to know if someone was a lesser risk than the algorithm predicted. In contrast, FICO does have reliable metrics to measure the accuracy of its risk assessments because it is easy to track whether someone does or does not pay back their credit.

Through this analysis, it is apparent that other predictive policing programs will have many of the problems inherent to the Secure Flight program because of the difficulties in defining a proper baseline, correcting inaccurate data, and verifying the prediction. In order to have a proper baseline to predict whom within a society will commit crime, police departments will need to collect information on every citizen, much like FICO. This, of course, is rife with privacy concerns as well as civil rights and civil liberties issues. In order for predictive policing programs to avoid the same issues as Secure Flight, they must create and maintain viable and effective redress programs that allow citizens to question and correct the data that the programs utilize.

Ultimately, predictive policing programs must find accurate metrics. Most programs rely on crime rates as the metric to measure success; however, dropping crime rates are not enough to determine accuracy of risk analysis.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my wonderful fiancé, Michael Wittke, for his unending support. His faith in me helped me stretch farther than I thought I could stretch. I would also like to thank my mom for planning my wedding, which freed me to write this thesis.

Next, I would like to thank my two advisors, Rodrigo Nieto-Gomez and John Rollins, for their support, critiques, and comments, which made this thesis much stronger.

Last, but not least, I would like to thank my wonderful classmates in Cohorts 1501 and1502. I am truly humbled and in awe by all they do to serve our country and support one another. I am blessed to have them in my life.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

One of the more contentious uses of big data analytics in homeland security is predictive policing, which harnesses big data to better allocate police resources, decrease crime, and increase public safety. It is a tool "that develops and uses information and advanced analysis to inform forward-thinking crime prevention."[1]

Predictive policing began by predicting crime locations by relying on crime statistics and other data.[2] By analyzing the data, predictive policing models forecast where there might be an increase in certain types of crimes—especially property-related crimes.[3] Recently, however, law enforcement has begun to use predictive policing to assist in predicting which individuals may be likely to commit criminal activities,[4] essentially giving individuals a FICO score for how likely they are to commit a crime rather than how likely they are to pay back a loan. This expansion in predictive policing and the world of opportunity that comes with it has piqued the interest of homeland security experts, who hope that big data can be used to predict human behavior. However, predicting human behavior is rife with difficulty.

Government attempts to collect large amounts of data on American citizens is not revolutionary. The government has sought to collect data on Americans since the first Census on August 2, 1790.[5] In fact, data has been used for public safety efforts since the 1800s, when Dr. John Snow mapped cholera clusters in London that showed how the

---

[1] Craig D. Uchida, *A National Discussion on Predictive Policing: Defining Our Terms and Mapping Successful Implementation Strategies*, (Report No. NCJ 230404) (Washington, DC: National Institute of Justice, 2009): 1.

[2] Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion," *Emory Law Journal* 62 (2012): 259, 265.

[3] Nate Berg, "Predicting Crime—LAPD Style," *Guardian*, June 25, 2014, http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report.

[4] Ferguson, "Predictive Policing and Reasonable Suspicion," 266.

[5] "When Was the First Census in the United States?," U.S. Census Bureau, accessed Aug. 22, 2016, https://www.census.gov/history/www/faqs/demographic_faqs/when_was_the_first_census_in_the_united_states.html.

disease spread and opened the door to improved medical techniques.[6] What is revolutionary about modern-day data collection is the amount of data that is collected and stored, and the increased computational capacity by both government and private entities to aggregate and analyze the data about each individual.

Technological advances have made it easy and inexpensive to create, collect, store, and analyze all types of data. It is estimated that in 2019, it will take "an individual more than five million years to watch the amount of video that will cross global [internet protocol (IP)] networks each month."[7] Furthermore, as the growth of the "internet of things"[8] continues, so does the amount of accessible personal data available for analysis.[9] This profusion of data will continue to span a wide spectrum. Some of that data will be about the mundane trivialities of life—what time your coffee maker is set to start—to very personal data—what time you remind yourself to take certain medications.[10] It is these technological breakthroughs in big data analytics that law enforcement departments hope to harness through predictive policing programs.

For some departments, that hope has already been realized. For example, the Chicago Police Department used predictive policing to assemble a list of roughly 400 individuals who are likely to be involved in violent crime.[11] The "heat list," as the Chicago Police Department calls it, is compiled by using data points that included

[6] John Podesta et al., *Big Data: Seizing Opportunities, Preserving Values* (Washington, DC: Executive Office of the President, May 2014).

[7] "The Zettabyte Era—Trends and Analysis," Cisco, June 2016, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.

[8] Jacob Morgan, "A Simple Explanation of 'The Internet of Things,'" *Forbes*, May 13, 2014, http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#15c4d0d16828.The Internet of things (IoT) is the concept of connecting any type of electronic device to the internet. This allows for a significant increase in the number of devices that can collect information about individual's daily moments.

[9] "United States of Emoji," SwiftKey, accessed Aug. 31, 2016, http://swiftkey.com/en/united-states-emoji/#. Big data analytics can even predict which emoji you are more likely to use based on your geography.

[10] Podesta, *Big Data*, 2.

[11] Ibid., 31.

information about individuals' criminal records, social circles, and gang connections.[12] Police officers then use the heat list to visit the individuals and warn them that they were being closely watched.[13] Similarly, Kansas City, Missouri, began the Kansas City No Violence Alliance, which also uses predictive policing to forecast individuals who are likely to commit violent crimes. Those individuals are also asked to attend a meeting in which they are told they are being watched by law enforcement and that "the next time they, or anyone in their crews, commit a violent act, the police will come after everyone in the group for whatever offense they can make stick, no matter how petty."[14]

Additionally, police officers in Philadelphia predict which parolees are more likely to be recidivists.[15] The Philadelphia program uses big data analytics in order to assess each new parolee as a low-risk, moderate-risk, or high-risk case.[16] Through this model, Philadelphia has been able to allocate the correct amount of resources for each case.[17] The Los Angeles Department of Children and Family Services has also begun testing the use predictive policing to determine which children in its care are at a higher risk of suffering abuse. Like the Philadelphia parole program, the hope is that overworked social workers can more easily identify the urgent cases and focus their time and energy on those cases.[18]

These four programs focus on improving resource allocation, but they also bring significant implications for civil rights and liberties. Each program makes risk

---

[12] John Eligon and Timothy Williams, "Police Program Aims to Pinpoint Those Most Likely to Commit Crimes," *New York Times*, Sept. 25, 2015, http://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html?_r=0.

[13] Michael Thomsen, "Predictive Policing and the Fantasy of Declining Violence in America," *Forbes*, June 30, 2014, http://www.forbes.com/sites/michaelthomsen/2014/06/30/predictive-policing-and-the-fantasy-of-declining-violence-in-america/#353047606931.

[14] Eligon and Williams, "On Police Radar for Crimes They Might Commit."

[15] Ibid.

[16] Nancy Ritter, "Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise," *National Institute of Justice Journal*, 271(February 2013), http://www.nij.gov/journals/271/pages/predicting-recidivism.aspx.

[17] Ibid.

[18] Andrea Gardner, "Can an Algorithm Predict Child Abuse? L.A. County Child Welfare Officials Are Trying to Find Out," Southern California Public Radio, January 13, 2015, http://www.scpr.org/news/2015/01/13/49191/can-an-algorithm-predict-child-abuse-la-county-chi/.

assessments about individuals, and those assessments are used to determine how to treat that individual. If the Chicago or Kansas City programs incorrectly forecast someone as a potential violent offender, then that person is closely monitored by the police for no reason. This wastes law enforcement resources as well as encroaches upon the civil rights and civil liberties of the individual. If the Los Angeles program incorrectly predicts that a child will be abused, then the families that receive higher scrutiny could face needless upheaval, which could have serious negative effects on the child's welfare. As with most tools, there are benefits, and there are detriments. The key is to ensure that the correct balance is struck.

In order to uphold accuracy, big data analytics often rely on the "four Vs"—volume, velocity, variety, and veracity.[19] Volume requires a large amount of data, velocity requires that the data be added and processed at high speeds, and variety requires that the data come from multiple sources. Some authors argue that big data must also be accurate, which has become known as the fourth V, veracity.[20] It becomes apparent that veracity is especially important when attempting to predict how a particular person will act. Given the significant implications of predicting human behavior, I argue that a fifth V should be added—verification. Thus, in order for a big data program to succeed, the five Vs must be met.

Understanding the type of data relied upon by the algorithm is important, especially given that the datasets relied on are often from third- and fourth-party providers.[21] Not all data is the same, thus where a predictive policing program procures the data is important. Without understanding the type of data and where the data comes from, predictive policing programs cannot ensure the veracity of the data used, nor can

[19] Chan and Moses, "Is Big Data Challenging Criminology?," 21, 24.

[20] Berk and Bleich, "Statistical Procedures for Forecasting Criminal Behavior," 513–544, as quoted in Chan and Moses, *"Is Big Data Challenging Criminology?,"* 28, stating that accuracy is important for big data analytics; for further discussion, see "The Four Vs of Big Data," IBM Big Data &Analytics Hub, accessed Aug. 12, 2016, http://www.ibmbigdatahub.com/infographic/four-vs-big-data.

[21] Andrew Guthrie Ferguson, "Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards," *Oklahoma Law Review* 66 (2014): 831–874.

they ensure that the combination of datasets produce accurate results.[22] By using the data collected by third or fourth parties, it may also be difficult to secure corrections to inaccurate information.

The Privacy Act of 1974 requires that the federal government reasonably ensure that the data it collects is correct and permits individuals to petition the federal government to correct inaccurate records.[23] However, even the Privacy Act has large gaps. In order for someone to seek a correction to his or her data, the individual must know what data the government has about them. Even with System of Records Notices (SORN), which describes federal data records, it can be difficult for individuals to know the sources and the type of data on file with the federal government. Additionally, unlike the federal government, which, in most cases, must publish a SORN private entities and states do not necessarily have the same requirement. This makes it significantly harder for individuals to correct their records. Thus, the onus to ensure accurate data falls on the predictive policing program, as the data steward, and the program should constantly check its records even though there is no legal requirement to do so. Continual updates to data will ensure that the data is accurate, and thus, that the predictions made are true.

For the most part, researchers tend to focus on the use of the analytics by the end user, which can be government entities, private entities, or individuals. Although an end user incorrectly using the prediction is troubling, sometimes the incorrect use is caused by a lack of understanding of the predictive analytics program.[24] Misuse also can come when a program does not properly verify the risk assessment—what I propose should be the fifth V. In order to protect civil rights and liberties and to ensure privacy, there should be guidelines for law enforcement to rely on when deciding how to use the risk assessments created by predictive policing. Additionally, there should be clear metrics to verify that the predictive policing program creates accurate risk assessments. By creating solid guidelines that incorporate the five Vs, law enforcement can ensure that the

[22] Latanya Sweeney, *Discrimination in Online Ad Delivery* (Cambridge, MA: Harvard University, Jan. 28, 2013), http://ssrn.com/abstract=2208240.

[23] The Privacy Act of 1974, 5 U.S.C. § 552a (1974).

[24] Chan and Moses, "Is Big Data Challenging Criminology?," 32; State v. Loomis, 2016 WL 3704814, (Supreme Court of Wisconsin 2016).

predictive policing programs do not harm civil rights and liberties, nor waste police resources.

Luckily, predictive policing is not the government's or private companies' first attempt to use predictive analytics to predict human behavior. Credit rating agencies, through FICO scores, use big data analytics to predict who will repay their loans. More recently, the Transportation Security Administration (TSA) started tapping big data analytics in its attempts to predict who will be low-risk airline passengers. Predictive policing can learn from the mistakes and successes of these two programs.

B. RESEARCH QUESTION

What are the challenges of adopting effective predictive policing technologies and policies that provide benefits to law enforcement while protecting the privacy and civil rights and liberties of individuals?

C. RESEARCH DESIGN

This research harnesses a combination of legal review and case studies. First, I review the current legal environment within the United States for predictive analytics programs, in order to understand how these laws, regulations, and guidelines will apply to a predictive policing program. Next, I will perform a case study by reviewing the Secure Flight and FICO score programs. By analyzing the common pitfalls of these programs and applying them to predictive policing, potential problems can be avoided.

II. LITERATURE REVIEW

There are several federal laws that cover how data can be collected, and then once collected, used, by the federal government.[25] However, there are very few laws that dictate how a program that relies on big data analytics should create its database or use the predictions.

A. PRIVACY ACT

Federal agencies must follow the requirements of the Privacy Act when collecting or storing data. The Privacy Act lays out the requirements that each agency must follow when maintaining a system of records. Because any system relied upon for predictive policing programs would be a system of record, the federal agency will need to follow all 12 requirements, unless the database is exempted from the requirements. This literature review will discuss only the requirements that most directly affect big data collection.

5 U.S.C. § 552a(e)(1) requires agencies to "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency."[26] What is relevant and necessary will depend on the particular agency's statutory authorities.[27] Thus, the reasons to collect data can be broad, especially if the program's mission is to predict future crime. Any information that would be necessary and relevant to accurately predict who will commit crime could be included in a predictive policing program.

5 U.S.C. § 552a(e)(5)[28] requires agencies to maintain the records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure

[25] I chose not to include the Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000-ee3 because it only requires federal agencies to report their data mining activities to Congress; it does not control, condition, or limit those activities.

[26] 5 U.S.C. § 552a(e)(1).

[27] Reuber v. United States, 829 F.2d 133, 139–140 (D.C. Cir. 1987).

[28] Note 5 U.S.C. § 552a(e)(5) is one of the sections in which the head of an agency may exempt a system of records from adhering to its requirements. This exemption is only available to the Central Intelligence Agency or other agency that performs "as its principal function any activity pertaining to the enforcement of criminal laws." For further discussion, see 5 U.S.C. § 552a(j).

fairness to the individual in the determination."[29] This section does not require perfection, instead the courts created a reasonable standard for agencies to follow.[30] As the Court of Appeals for the Seventh Circuit noted, "the Privacy Act merely requires an agency to attempt to keep accurate records, and provides a remedy to a claimant who demonstrates that facts underlying judgments contained in his records have been discredited."[31] Thus, an agency must take reasonable measures to ensure the accuracy of the data maintained in the database.

5 U.S.C. § 552a(e)(7) requires that an agency does not maintain any records "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual … or pertinent to … an authorized law enforcement activity."[32] The Office of Management and Budget (OMB) guidance on the Privacy Act encourages agencies to use a broad, reasonable interpretation as to what types of activities constitute exercising a right under the First Amendment.[33] This is extremely important to understand when creating a predictive analytics database. Often surveillance can include information on an individual's religious beliefs, political beliefs, and associations.[34]

5 U.S.C. § 552a(e)(9) and (10) require that agencies establish "rules of conduct for persons involved in the design, development, operation, or maintenance"[35] of the system of records and "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records."[36] This pertains to records that are leaked or hacked. The legal liability under this section could mean a class

[29] 5 U.S.C. § 552a(e)(5).

[30] Johnston v. Horne 875 F.2d 1415, 1421 (9th Cir. 1989).

[31] Debold v. Stimson, 735 F.3d 1037, 1040–41 (7th Cir. 1984).

[32] 5 U.S.C. § 552a(e)(7). Unlike 5 U.S.C. § 552a(e)(5), this section cannot be exempted under 5 U.S.C. § 552a(j).

[33] 40 Fed. Reg. 28,965 (July 9, 1975).

[34] Maydak v. U.S., 363 F.3d 512, 516 (D.C. Cir. 2004), finding "it obvious that photographs of prisoners visiting with family, friends, and associates depict the exercise of associational rights protected by the First Amendment."

[35] 5 U.S.C. § 552a(e)(9).

[36] 5 U.S.C. § 552a(e)(10).

action lawsuit of individuals harmed by any unintentional release of records and could be costly for the agency. Thus, cybersecurity concerns should be treated seriously.

Along with statutes, the Office of Management and Budget (OMB) issued several memoranda to guide federal agencies in the sharing and use of data. OMB published the memoranda in response to Executive Order 13,642 and, like the executive order, it encourages interoperability and openness. However, the memoranda also encourages the protection of the data and assurance that data is collected and used only when necessary and relevant to achieve an agency's missions.

The OMB memorandum that is most relevant is the "Guidance for Providing and Using Administrative Data for Statistical Purposes" because predictive analytics programs at their core are statistics-based programs. Generally, the memorandum requires statistical agencies to be good data stewards, appropriately managing data through its life cycle, entering into interagency agreements before accepting the data, and protecting its privacy.[37]

B. FOURTH AMENDMENT

The rise of predictive analytics will have a several effects on Fourth Amendment jurisprudence. First, more information will be collected on individuals in police databases, and those individuals may not receive notice of the collection.[38] Without notice, individuals will never have the ability to challenge the collection and dissemination of their information or have the opportunity to correct potentially erroneous data. Notice is a foundational element to the Fourth Amendment. Before the rise of electronic searches, notice was a given because individuals tend to notice when their homes, personal effects, and persons are being physically searched.[39] Now,

[37] Office of Management and Budget, "Memorandum for the Heads of Executive Departments and Their Agencies: Guidance for Providing and Using Administrative Data for Statistical Purposes" (M-14-06), Feb. 14, 2014, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-06.pdf.

[38] Patrick Toomey and Brett Max Kaufman, "The Notice Paradox: Secrete Surveillance, Criminal Defendants & the Right to Notice," *Santa Clara Law Review* 54 (2014): 843–900.

[39] Ibid.

however, a person may never realize that the government searched or seized their electronic files.[40]

Furthermore, predictive analytics may change a police officer's or judge's evaluation of reasonable suspicion and probable cause. Both reasonable suspicion and probable cause rely on the analysis of the totality of the circumstances. As predictive analytics begins to predict who is more likely to commit a crime, the predictions could become an element in a totality-of-the-circumstances evaluation.[41] Thus, the analysis will depend on the datasets that are included in the database. For example, if the database relies on past criminal record, current neighborhood, groups the person joins, and schools attended for an evaluation, the analysis will begin to rely on information that police and courts have rarely been able to use before to determine reasonable suspicion. Instead of analyzing just the circumstances of the situation at hand, a person's entire background will also be a factor, for the first time. Therefore, fully understanding and scrutinizing the types of data that are included in the databases will be incredibly important to the protection of constitutional rights.

C. FICO

The Fair Isaac Corporation was founded in 1956 and provided one of the first analytic solutions for credit ratings.[42] The FICO score algorithm is a secret, like most predictive analytic programs, and is relied upon by the three major U.S. credit agencies, Experian, Equifax, and Transunion.[43] Most individuals understand that their credit worthiness is based on their FICO score; however, many Americans are surprised when their FICO score is also used to determine their status in other areas of their life. For instance, many employers use the FICO score to screen applicants and help assess whether he or she will be a good employee, and insurance companies use FICO scores to

[40] Ibid.

[41] Andrew Guthrie Ferguson, "Big Data and Predictive Reasonable Suspicion," *University of Pennsylvania Law Review* 163 (2015): 327–428; Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion," *Emory Law Review* 62 (2012): 259.

[42] "FICO at a Glance," FICO, accessed Feb. 6, 2016, http://www.fico.com/en/about-us#at_glance.

[43] Shweta Arya, Catherine Eckel, and Colin Wichman, "Anatomy of the Credit Score," *Journal of Economic Behavior & Organization* 95 (2013): 175–185.

determine insurance rates.[44] There is even an online dating website that primarily relies upon an individual's credit score to determine whether the person will be a good life partner.[45] Thus, what started as an instrument to help banks determine creditworthiness became a tool used to assess and define much more about a person.

As with most tools, FICO's has both supporters and detractors. In "Anatomy of the Credit Score," Arya, Eckel, and Wichman summarize much of the literature that determines that FICO Scores correlate to trustworthiness, patience, and loan repayment.[46] They also, through their own work, suggest that credit scores correlate to "impulsivity, time preference (or future orientation), and trustworthiness."[47] Thus, FICO can be used as an accurate indicator of certain human characteristics.

However, many studies also suggest that U.S. credit bureaus contain significant errors. For example, Smith et al. summarize the literature that expresses doubts about FICO scores' accuracy.[48] In the same paper, they also conducted a study that sampled 1,000 U.S. consumers and reviewed their credit reports from the three bureaus. Out of those records studied, 26% included at least one material error.[49] An interesting aspect of their study is that they also followed those individuals as they attempted to correct the errors. Only 78% of those individuals were able to get at least one bureau to alter their credit rating.[50] These alterations often made significant differences to the credit scores. The authors' concluded that credit scores can be a good indicator of creditworthiness, but only if consumers are vigilant to ensure that the data included in their score is accurate.[51]

---

[44] Ibid.; for further discussion, see Bernerth et al., "An Empirical Investigation of Dispositional Antecedents and Performance-Related Outcomes of Credit Scores," *Journal of Applied Psychology* 97, (2012): 469–478, studying whether FICO scores should be used as an employment indicator.

[45] "About," Credit Score Dating, accessed Feb. 6, 2016, http://creditscoredating.com/.

[46] Arya, Eckel and Wichman, "Anatomy of the Credit Score," 176.

[47] Ibid., 184.

[48] Smith et al., "Accuracy of Information Maintained by U.S. Credit Bureaus: Frequency of Errors and Effects on Consumers' Credit Scores," *The Journal of Consumer Affairs* (Fall 2013): 589–590.

[49] Ibid., 593.

[50] Ibid., 594, 600, noting that because consumers had the assistance of the researchers in filing their disputes, the participants in this study may have had more success than other consumers.

[51] Ibid., 600.

D. SECURE FLIGHT

Secure Flight began in 2009 to identify airline passengers who posed a high security risk by comparing passenger lists against federal government watch lists.[52] In 2011, the program expanded to include lists of pre-approved low-risk travelers, such as those in the Transportation Security Administration Precheck program. Secure Flight's objective eventually evolved to include risk analysis for individuals on a per-flight basis to determine their general risk to aviation security. The risk assessment is determined from passenger name records (PNR), government watch lists, such as the No Fly List and the Terrorist Screening Database, and other databases. All data is destroyed within seven days of the flight and is only kept if a passenger complains that he or she was wrongly identified under the system.[53]

Even after a few years in operation, the possibility of being wrongly identified by the system is possible. At least two of the databases that the Secure Flight program accesses, the Terrorist Screening Database (TSDB) and the No Fly List, have struggled with the accuracy of data. Not only have the databases struggled with delivering accuracy, but the programs have also struggled with creating an effective redress program. The recent litigation surrounding the No Fly List highlights the lack of constitutionally required due process for both databases.[54] Thus, a significant issue to consider when creating a predictive policing program is the proper redress for individuals who are incorrectly included. To achieve this will be difficult because, much like the Secure Flight program, full transparency could jeopardize ongoing law enforcement investigations. Consequently, learning from the mistakes made with TSDB and the No Fly List could prevent wasted police resources, increase community trust, and ensure that civil rights and civil liberties are effectively protected. This issue also points to a problem with the common practice of relying on third- or fourth-party data providers because it is

[52] Government Accountability Office (GAO), *TSA Has Taken Steps to Improve Oversight of Key Program, but Additional Actions Are Needed* (GAO-15-559T) (Washington, DC: GAO, May 13, 2015), 3.

[53] "DHS/TSA-019 Secure Flight Records System of Records," 233, 238.

[54] Latif v. Holder, 28 F. Supp 3d 1134, 1161–62 (D. Or. 2014), finding the TSA redress procedures did not meet the constitutional for due process; Ibrahim v. Dept. of Homeland Security, 62 F. Supp. 3d 909, 931(D. N. Ca. 2014), finding that TSA did not provide constitutional due process to plaintiff.

extremely difficult to ensure accuracy and whether providers have procedures to permit people to correct inaccurate data.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PREDICTIVE ANALYTICS: HOW NETFLIX LURES YOU INTO ANOTHER MARATHON WATCHING SESSION

The basic definition of predictive analytics is "technology that learns from experience (data) to predict the future behavior of individuals in order to drive better decisions."[55] Prior to big data analytics, most statistical forecasts were made based on samples. Today, however, massive amounts of data are collected on individuals every day, so scientists, businesses, and government can make forecasts based on extremely large amounts of data. Analytics have improved because the forecasts are no longer based on small samples but on the analysis of an entire universe of data.

In a fundamental sense, predictive analytics relies on an algorithm (written by humans) to learn from data (collected from humans), to predict actions (of humans). As anyone who has lost a thesis by inadvertently striking a wrong key during a late night writing session can confirm, sometimes the weakest point of any software program is human involvement. Thus, the weakest part of the predictive analytics program is in the data and the algorithm. If the collected data is wrong, out of date, or illegible to the program, then that data will lead to the wrong prediction. If the technician writing the algorithm makes the wrong assumptions or puts too little or too much weight on certain data, then the algorithm will make a wrong prediction.

A. DATA

Predictive analytics programs are able to search for connections, or needles in the haystack, (formally known as statistically significant anomalies or variations), that scientific and human analysis were unable to find before the ability to analyze each piece of hay.[56] However, in order for this to work, the predictive analytics program must collect the whole haystack (formally known as the baseline). If the predictive analytics program relies on too little data, then it runs into the same problems that sampling runs

[55] Eric Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die* (Hoboken, NJ: John Wiley & Sons, 2016), 14.

[56] Siegel, *Predictive Analytics*, 87.

into. Even so, just having the haystack does not equate to a perfect prediction. The type of data used in predictive analytics requires what has become known as the three Vs—volume, velocity, and variety.[57] Volume requires a large amount of data, velocity requires that the data be added and processed at high speeds, and variety requires that the data be from multiple sources. Some authors argue that data must also be accurate, which has become known as the fourth V—veracity.[58] Therefore, in order for a predictive analytics program to succeed, at the very least, the four Vs must be met.

Volume, as mentioned above, is about collecting the whole haystack, and there can be significant concerns about this collection. The data that is collected about individuals and sold for about a half a cent, describes some of an individual's most intimate decisions.[59] Predictive analytics can predict employees who will quit their jobs, what ads consumers are likely to click on, which insured person is most apt to die, and whether a woman is pregnant.[60] These predictions come from collections of data from both the government and private companies. Because of this, there is a negative gut reaction to the idea that the police will collect significant amounts of data on all citizens. Nonetheless, in order for a predictive analytics program to be able to recognize that something is a needle as opposed to a piece of straw, it must have the entire haystack to analyze. The anomalies, or the needle, only become apparent when the algorithm understands what is the normal baseline.[61]

This same analysis can be applied to the second V—variety. If a predictive program does not have enough variety of data, then the analysis will not be accurate. To continue the beleaguered analogy, the predictive program needs to know what every type

---

[57] Chan and Moses, "Is Big Data Challenging Criminology?," 21, 24.

[58] Berk and Bleich, "Statistical Procedures for Forecasting Criminal Behavior," as quoted in Chan and Moses, "Is Big Data Challenging Criminology?," 28, stating that accuracy is important for big data analytics; see also "The Four Vs of Big Data" http://www.ibmbigdatahub.com/infographic/four-vs-big-data.

[59] Alexis Madrigal, "How Much Is Your Data Worth? Mmm, Somewhere between Half a Cent and $1,200," *Atlantic*, March 19, 2012, http://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/.

[60] For more information, see Siegel, *Predictive Analytics.*

[61] Siegel, *Predictive Analytics,* 87.

of straw could possibly look like in order to tell when something is not a straw. It also needs to know what all needles look like in order to tell if something is just a bug. Conversely, there is a possibility of using too many data points.[62] Thus, the art of predictive analysis is finding the point when the variety of data points maximizes the analysis because too little or too many will cause bad predictions.

Stale data creates stale predictions. As such, the velocity in which the data is updated is extremely important to a predictive analytics program.[63] This also affects the accuracy, or veracity, of the data, the fourth V. Understanding the type of data relied upon by the algorithm is also important, especially given that the datasets relied on are often from third- and even fourth-party providers.[64] Without this understanding, predictive policing programs cannot ensure the veracity of the data used nor can they ensure that the combination of datasets produce accurate and not discriminatory results.[65] By using the data collected by third or fourth parties, it will also be difficult for the programs to correct inaccurate information.

B. ALGORITHMS

Algorithms are incredibly powerful tools and the people who write the code have an awesome responsibility. Algorithms are so powerful that they have entered the political realm, as is indicated by a conference in June 2016 that was dedicated solely to the politics of algorithms.[66] As Gillespie explains, algorithms should not be viewed only as technological achievements, rather we "must unpack the warm human and institutional

[62] Siegel, *Predictive Analytics*, 143.

[63] Ying Lie, "Big Data and Predictive Business Analytics," *Journal of Business Forecasting* (Winter 2014–2015): 40–42.

[64] Ferguson, "Big Data Distortions," 66.

[65] Sweeney, *Discrimination in Online Ad Delivery*, 34–35.

[66] "Preconference Call for Papers: Algorithms, Automation and Politics" International Communication Association, accessed Aug. 2, 2016, http://www.icahdq.org/conf/2016/AlgorithmsCFP.asp; for further discussion, see also Project Bots, A Project Algorithms, Computational Propaganda, and Digital Politics, http://www.politicalbots.com/.

choices that lie behind these cold mechanisms."[67] Take, for example, Google's search code. It determines what hits you see when you search for something to cook for dinner or when you google the name of your date from that credit score dating website. With one stroke of the button, though, Google can change what information comes up top and what information becomes your 100th hit. Google has, in fact, done this when it decided to down-weight (or de-emphasize) any hits that came from mug shot websites.[68] Now, a potential date's mug shot will not be one of the first hits that surfaces when a dating hopeful conducts a search before deciding whether to accept an invitation for drinks.

Inherent in every algorithm are criteria that are used to rank the data. These criteria "essentially embed a set of choices and value propositions that determine what gets pushed to the top of the ranking."[69] These choices are a type of 21st century art. The programmers make significant choices when creating their algorithms including the type of data analyzed, the weight in the algorithm that each data set receives, and the acceptable level of false negatives and positives. Thus, their subconscious assumptions and biases can greatly affect the predictive outcome.[70] Often, though, the value determinations are not readily available to the public. Hence, society never gets to determine whether the value determinations made by a handful of programmers fit the values of that society. Take Google's decision to down-weight mugshots in their search algorithm. Google determined that the privacy of an arrestee who may never have been convicted outweighs the curiosity about one's neighbors. It is a value judgment. This is even more troubling for algorithms used by governments to predict the actions of citizens and thus determine how the government will treat that citizen.

---

[67] Tarleton Gillespie, "The Relevance of Algorithms," in *Media Technologies: Essays on Communication, Materiality, and Society*, eds. Tarleton Gillespie, Pablo Boczkowski, and Kirsten Foot (Cambridge, MA: MIT Press, 2014). http://mixedrealitycity.org/readings/Gillespie_TheRelevanceofAlgorithms.pdf.

[68] Nicholas Diakopoulos, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes* (New York: Columbia Journalism School, Tow Center for Digital Journalism, Dec. 3, 2014), 2, http://towcenter.org/research/algorithmic-accountability-on-the-investigation-of-black-boxes-2/.

[69] Diakopoulos, *Algorithmic Accountability Reporting*, 5.

[70] Tal Z. Zarksy, "Transparent Predictions," *University of Illinois Law Review* (2013): 1503, 1517–1518.

It is because of this awesome power that the Vs of predictive analytics should not just cover the big data used. Rather, there should be a fifth V—verification. Verification requires that the prediction be verified as accurate. It verifies that the mixture of data chosen and the value judgments of the algorithm create an accurate prediction. This is usually accomplished through a two-step process.[71] A set of data with a known output is split into a training set and a testing set. The training set is used to train the algorithm. The algorithm then analyzes the testing set, and if all goes well, the algorithm makes the correct prediction. However, even after this initial testing, the algorithm must be continually tested to ensure that it has not gone stale.[72]

The continued testing of some predictive analytics programs is rather simple. When predictive analytics is used to forecast whether a consumer is pregnant, there is a way to verify that guess when the consumer begins buying diapers in nine months. You know if the Netflix algorithm is off when you have no desire to watch any of the shows it recommends. When the FICO score predicts the likelihood that someone will not default on a loan, the prediction is tested by tracking whether the individual fulfills his or her financial obligations. However, predictive policing is attempting to predict a negative, and that is difficult to verify.[73] For example, if a predictive policing program predicts that an individual will commit crimes once released from prison, and the government does not release the convict, the program's guess cannot be verified. It is not hard to imagine the scene from *1984* when Parsons is thrown into prison with Winston. Parson states that he is an agent of Goldstein, but he did not know it.[74]

Managing all of these issues is not easy. Finding the right balance of volume, variety, and velocity is an art. Ensuring the veracity of data and verifying the predictions is time consuming. Furthermore, in some instances, it is impossible to verify the

[71] Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (Santa Monica, CA: RAND, 2013), 41.

[72] Perry et al., *Predictive Policing,* 13.

[73] Siegel, *Predictive Analytics*, 70.

[74] George Orwell, *1984* (New York: Signet Classics, 1949), 232–34.

prediction, which limits one of the most important aspects of predictive analytics—machine learning.

This balance is especially difficult for predictive policing programs. Determining which datasets to use to predict who will commit a crime means deciding which theories regarding criminal behavior to follow. After determining which datasets to include, the coder must determine which datasets are more likely to predict who will be a criminal and ensure that the algorithm weighs that factor more than the others. The coder must somehow create concrete metrics to verify that the predictions are correct. Finally, the accuracy and completeness of the data must be maintained and the predictions continually tested to ensure the algorithm has not gone awry. Obviously, creating the criminal FICO score is not a simple proposition.

IV. PREDICTIVE POLICING: YOUR CRIMINAL FICO SCORE

A. CREATING THE PREDICTIVE POLICING PROGRAM

Predictive policing has been defined broadly by the National Institute of Justice as "any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention."[75] Predictive policing can be as simple as heuristic methods to complicated predictive analytics.[76] The goal for any predictive policing program is to prevent crime by predicting where crime is likely to occur or who is likely to commit crime. Thus, the specific goal of the program will affect which predictive analytics methods are chosen.[77] The goal of the first-generation predictive policing programs was simply to determine *where* crime was most likely to be committed. Today, cutting-edge predictive policing programs ask *who* is likely to be involved in crimes. Those are very different goals with very different methodologies.

After determining the goal of a predictive policing program, the algorithm must be created.[78] The algorithm and the methods used to create the algorithm will depend on the amount and type of data, the question, and the resources of the particular police department.[79] The method can be as simple as data mining and geomapping to as complicated as social networking analysis.[80] The bottom line, though, is that each method's goal is to predict human behavior.

After choosing the method to be used, the programmer determines what data is needed and how it should be collected. This is not an easy process for police departments, analytics experts, or computer programmers. As the internet of Things grows,

---

[75] Uchida, *A National Discussion on Predictive Policing*, 1.

[76] Perry et al., *Predictive Policing,* 17–55. For this thesis, I narrow the focus to the predictive policing programs that involve predictive analytics.

[77] Siegel, *Predictive Analytics*, 24.

[78] For a comprehensive review of the various forms of predictive analytics, see *Predictive Policing* by Perry et al. For the purposes of this thesis, it is enough to know that there are several methodologies that can be used by a predictive policing program.

[79] Perry et al., *Predictive Policing,* 11–15.

[80] Ibid., 101–107.

departments have more and more data from which to choose.[81] In fact, third-party data providers continue to grow as data providers for law enforcement.[82] This data can be defined as open source, such as the information found on Twitter,[83] or it can be more sensitive, such as data from financial records.[84]

Thus, the programmer has a wealth of data from which to choose and must determine what data will and will not be used by the algorithm. Most investigatory information will come directly from the police department.[85] However, information about demographics and other environmental data will come from third- or fourth-party vendors.[86] Not only does the programmer need to choose which data to use, but the programmer must also assess the accuracy of that data. Data obtained directly from a police department or a third or fourth party has the possibility of including significant errors.[87] An error can be caused by case notes that were not properly translated into machine-readable data or by incorrect or stale data.[88] A police officer might think Bob and Susie are dating when in reality, Bob is dating Susie's friend, Jane. Or, the case notes were not updated to reflect that Bob is now dating Linda, and Jane and Susie are no longer friends with Bob or Linda. All are easy mistakes to make, but these mistakes will cause the predictive algorithm to make incorrect predictions. Third- and fourth-party data providers experience similar issues, but these are harder to correct because the source of the data is not always known.

---

[81] Morgan, "A Simple Explanation." The Internet of things (IoT) is the concept of connecting any type of electronic device to the internet. This allows for a significant increase in the number of devices that can collect information about individual's daily moments.

[82] Stephanie K. Pell, "Systematic Government Access to Private-Sector Data in the United States," *International Data Privacy Law* 2 (2012): 245.

[83] Christopher S. Stewart and Mark Maremont, "Twitter Bars Intelligence Agencies from Using Analytics Service," *Wall Street Journal*, May 8, 2016, http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682.

[84] Pell, "Systematic Government Access," 253.

[85] Perry et al., *Predictive Policing,* 13.

[86] Pell, "Systematic Government Access," 253.

[87] Perry et al., *Predictive Policing,* 13.

[88] Ibid.

After determining the data that should be used and collected, the data must then be converted into machine-readable data. This process, known as data fusion, is complicated even when only attempting to combine data about things. Data fusion becomes significantly more difficult when combining data about people, especially information collected from documents like case notes (not all law enforcement officers have easy-to-read handwriting). As with the predictive analytics methodology, there are several methods for data fusion. The programmer must determine the best method for the type of data chosen.[89]

Moreover, not only must the programmer choose from a wealth of data, but the programmer also must choose the weight that each data set receives. It is important to remember that "each algorithm is premised on both an assumption about the proper assessment of relevance, and an instantiation of that assumption into a technique for (computational) evaluation."[90] Thus, a programmer's own philosophical views on crime may play a role as to which datasets receive more weight.[91] There is a long history of research on what causes people to commit crime, and which theories the programmer opts to follow will change the type of data the programmer chooses to use and the weight that each dataset receives within the algorithm.[92]

At the end of this complicated process, a computer produces a score that represents a risk analysis. However, these assessments will not have the precision of say, the supercomputer in *Willy Wonka and the Chocolate Factory*, which could tell the exact location of the golden tickets.[93] Rather, the score forecasts the likelihood that a particular

[89] For a comprehensive discussion on the various data fusion methods and their complications, see Perry et al., *Predictive Policing*, 89–96.

[90] Gillespie, "The Relevance of Algorithms."

[91] Ibid.

[92] Perry et al., *Predictive Policing*, 41–42, 76, 78–79. For example, one study suggests that hotter temperature leads to more crime. Other researchers argue that burglars tend to stay within a certain area, gang shootings incite retaliatory violence, foreclosures lead to increased crime, and increased traffic violations correlate with increased crime.

[93] "Willy Wonka-Golden Ticket Super Computer," YouTube video, 1:10, from *Willie Wonka and the Chocolate Factory* (1971), posted by mediaFace, March 16, 2010, https://www.youtube.com/watch?v=-VujGNQpRjQ. Hopefully, if we ever build such a computer, it will not refuse to give us an answer because "that would be cheating." And hopefully, it will not just give us the answer that will require us to build the computer to determine the question like in *Hitchhiker's Guide to the Galaxy*.

person will be involved in crime. It is not a precise measurement but a risk analysis. It is therefore a tool that should be used with caution.

B. MEASURING THE RISK ANALYSIS

Before using the predictive policing program, the risk analysis must be fully analyzed to understand the weaknesses of each algorithm.[94] Prison systems have had some success in determining the risk that a parolee will commit a crime once released. This risk assessment is then used by the parole officer and police to give more attention to the parolee.[95] One such model developed by Berk assesses the risk that a parolee will commit a homicide after he or she is released.[96] The accuracy, however, is limited because the risk analysis only accurately forecasts about eight future kills out of every 100.[97] Another study attempted to predict school-age boys in Pittsburgh who are more likely to be involved in homicide. The study found that it is possible "to predict violence in a community sample of boys" with a relatively low false negative error rate of 17.4% but a high rate of false positive errors of 86.6%.[98] Although the number of boys that ultimately were involved in homicide that the study missed was low, the number of those incorrectly predicted to be involved in homicides was high. Other metrics have been used to assess risk. For example, the Chicago Police Department in 2012, through social network analysis methods, showed that individuals who are co-arrested with a homicide victim are more likely to be killed as well.[99] This work may be proving somewhat accurate because the Chicago Police Department claims that so far in 2016, three out of four shooting victims were on the Strategic Subject List and 80% of those arrested were

[94] It is important to note that each predictive policing program has different weaknesses. The differences in data and algorithms create different problems.

95 Perry et al., Predictive Policing, 92.

96 Ibid.

[97] Ibid.

[98] Loeber et al., "The Prediction of Violence and Homicide in Young Men," *Journal of Consulting and Clinical Psychology* 73 (2005): 1074–1088. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.483.6423&rep=rep1&type=pdf

[99] Perry et al., *Predictive Policing*, 99.

also on the list.[100] However, these metrics were recently called into question by a newly released study by Saunders et al.[101] The study concluded that individuals are not more or less likely to become a victim of a homicide or a shooting than the study's comparative group; however, an individual is more likely to be arrested if he or she is on the list.[102]

As these examples show, the metrics to prove the effectiveness of predictive analytics programs are squishy. What I mean by this is that one cannot simply assess the number of people correctly included but must also assess the number of people incorrectly included (formally known as false positives) and those incorrectly excluded (formally known as false negatives).[103] However, when predicting potential criminals, program operators will never know a program incorrectly included someone until that person dies without committing a crime. Therefore, it is no surprise that predictive policing programs struggle with finding an appropriate metric.[104]

Predictive policing programs commonly use the crime rate to measure the accuracy of the forecasts, but this may not be an accurate metric.[105] First, a crime rate for only a specific area will not account for the crime simply moving to a different area because of increases in police patrols due to predictive policing. Therefore, at the very least, the crime rate must be calculated for an entire jurisdiction. Second, the crime rate does not account for the false positives. Incorrectly including people on the list will have no effect on a crime rate. And lastly, the crime rate may not account for false negatives

[100] Nissa Rhee, "Study Casts Doubt on Chicago Police's Secretive 'Heat List,'" *Chicago*, Aug. 17, 2016, http://www.chicagomag.com/city-life/August-2016/Chicago-Police-Data/.

[101] Jessica Saunders, Priscillia Hunt, and John S. Hollywood, "Predictions Put into Practice: A quasi-experimental Evaluation of Chicago's Predictive Policing Pilot," *Journal of Experimental Criminology* 12 (2016): 1–25.

[102] Saunders at al., "Predictions Put into Practice," 1–25. It is important to note that Chicago Police Department questions the study because it is based on the 2013 version of the program, and CPD claims that the 2016 version is stronger. For further discussion, see the news release by Chicago Police Department, "CPD Welcomes the Opportunity to Comment on Recently Published RAND Review," Aug. 17, 2016, http://4abpn833c0nr1zvwp7447f2b.wpengine.netdna-cdn.com/wp-content/uploads/2016/08/RAND_Response-1.pdf.

[103] Diakopoulos, *Algorithmic Accountability Reporting*, 6.

[104] Ibid., 28; see also Saunders at al., "Predictions Put into Practice," 1–25.

[105] Joe Newbold, " 'Predictive Policing,' 'Preventative Policing' or 'Intelligence Led Policing.' What is the Future?" Warwick Business School, Coventry, UK, 2015, 11.

either. Most predictive policing programs include an element of added police intervention.[106] The prevention can include increased patrols, hardening (or better protecting) of the potential targets, and increased community contacts.[107] Consequently, the decrease in crime may not be because of the prediction but rather the increased police intervention. Predictive policing needs to find better metrics.

C. CONTROLLING THE USE OF THE RISK ANALYSIS

After a predictive policing program chooses a method and data, and measures the accuracy of the program, then it must use the assessment. An obvious use is to allocate limited resources accordingly. For example, police officers can use assessments to save time in investigations by focusing on certain individuals, and parole officers can schedule high-risk individuals for more check-ins than low-risk individuals.[108] In a time of continual belt-tightening, any tool to help departments better focus their resources is welcomed, but if predictive policing is used incorrectly, it could waste resources. Assessments also can be used in reasonable suspicion or probable cause analysis.[109] However, if a program's analysis is incorrect, then a police officer may search or seize the wrong individual. Therefore, significant civil rights and civil liberties abuses can occur if the predictive policing program is not properly controlled.

Police must ensure that the risk analysis created by the predictive policing program is used correctly. It is surprising that given the power the government has to make an assessment and decision about a person's character, there are no laws that directly cover predictive analytics use by law enforcement. The Privacy Act governs the collection and sharing of data, but it does not govern the analysis of that data. Furthermore, the Privacy Act only affects the federal government and does not cover data

[106] Newbold, "Predictive Policing," 12.

[107] Ibid.; Perry et al., *Predictive Policing*, 57–80.

[108] John Eligon and Timothy Williams, "Police Program Aims to Pinpoint Those Most Likely to Commit Crimes," *New York Times*, Sept. 24, 2015, http://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html.

[109] Ferguson, "Predictive Policing and Reasonable Suspicion," 259, 274; Elizabeth E. Joh, "Policing by Numbers: Big Data and the Fourth Amendment," *Washington Law Review* 89 (2014): 35; see also Perry et al., *Predictive Policing*, 108.

collected and used by state and local governments and private entities. The Fourth Amendment does not fully protect our digital data either.[110] Courts are beginning to assess predictive programs used in sentencing, however.[111] These cases prompted courts to create limits and conditions for the proper use of predictive policing. Because sentencing requires judges to consider the totality of an individual's character and circumstances, courts may use similar limitations and conditions when analyzing the totality of the circumstances for the application of the Fourth Amendment. However, the courts, thus far, have not done this.

With little guidance for predictive policing, how can predictive policing programs be sure that they are wielding this powerful tool wisely? In the following sections, I analyze two programs that apply predictive analytics, FICO and Secure Flight, in order to identify the successes and mistakes of those systems. By learning from other predictive analytic programs, predictive policing programs can avoid common mistakes and replicate the successes.

[110] Joh, "Policing by Numbers," 35.

[111] State v. Loomis, 2016 WL 3704814, (Supreme Court of Wisconsin 2016)

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE FICO SCORE: HOW I DISCOVERED THAT THE CREDIT BUREAUS THOUGHT I WAS MARRIED TO MY DAD

A. HISTORY OF CREDIT RISK SCORES

The FICO score has an interesting history, and in many ways, it illuminates what is happening in predictive policing programs. William R. Fair and Earl J. Isaac founded Fair, Isaac & Company, Inc., in 1956 as a problem-solving organization.[112] The company's first foray into the emerging market of credits cards was to design a billing system for Conrad Hilton's *Carte Blanche*, which was distributed to the hotel chain's guests. It was from this interaction that Fair and Isaac began to work to assist credit providers in selecting their customers, and in 1958, the company installed the first commercially produced credit scorecards for American Investment of St. Louis, Louisiana.[113]

These first scorecards were simple and developed only for the credit provider's particular customer base.[114] The customer base became the baseline. The limited baseline was necessary for the rudimentary predictive analytics program that Fair, Isaac was creating for the first time. The initial question addressed by the rudimentary program was limited to whether the credit providers should give credit to the individual. Each company received a different scorecard for each city in order to create an appropriate baseline to screen consumers within that distinct population.[115] In order to create the scorecards, Fair, Isaac would send several employees to review the administrative files of that particular branch. Based on the historical administrative files, Fair, Isaac would create a scorecard that would predict the consumers most likely to repay their debt.[116] Of course,

[112] Martha Poon, "Scorecards as Devices for Consumer Credit: The Case of Fair, Isaac & Company Incorporated," *Sociological Review* (2007): 288.

[113] Poon, "Scorecards as Devices," 288–89.

[114] Ibid., 289.

[115] Ibid., 289–290.

[116] Ibid., 290–291.

the statistical theory was only as good as the data; thus the variety, volume, and veracity of data for the particular branch was the foundation of any good predictive scorecard.

As with any predictive analytics program, the analyst that created each scorecard had to make several strategic decisions about the data provided by the branches. The analyst had to decide which pieces of data should be included, the correct sampling number, and the correct files to include in the sample.[117] Once this data was chosen, the files were sent to part-time workers, who were often homemakers.[118] Much like today, this aspect of predictive analytics was not seen as very important. However, the home-coders who were paid a few cents per sample application, made some incredibly important decisions because they made the data usable. The home-coders created what is known today as data fusion by interpreting the various documents, including any bad handwriting, in order to convert the data into the standardized numerical codes needed for the analytic process to be read by machine.[119] Because no credit provider used the same forms, this work was often an art form in translation.

After the home-coders turned the information into usable data, the analysts had to create the model to process the data. In order to do this, the analysts had to determine the amount of weight to put on each dataset in order to receive an accurate forecast on which individuals should receive credit.[120] The final algorithm was non-transferable because it could be applied only to that lender's business.[121] Modern-day credit-score formulas are well established. The decisions on what data to include, how to fuse the data, and the weight of each dataset has largely been determined; but nearly 60 years ago, designing the data set was an art in progress. The current environment of predictive policing is comparable to this stage of the FICO score's creation.

Fair, Isaac continued to build its business, and in the 1980s, the company began to change the data that it relied on to create algorithms. Instead of basing the algorithms on

[117] Ibid., 290.

[118] Ibid.

[119] Ibid.

[120] Ibid., 292.

[121] Ibid.

the files from specific lenders, Fair, Isaac began relying on the credit bureaus for the data.[122] With the ability to rely on a larger swath of consumer data, Fair, Isaac was able to develop an algorithm that could be applied nationwide.[123] This contemporary FICO score significantly changed how credit was given and used by individuals. Instead of waiting for a consumer to apply for credit and then evaluating his or her creditworthiness, banks and lenders, for the first time, could evaluate the general population of consumers and determine who should receive advertising to encourage him or her to apply for credit. This opened the door to a much wider market because lenders could now initiate credit relationships through advertising.[124]

Today, three major U.S. credit agencies, Experian, Equifax, and Transunion, rely upon the secret algorithm used for FICO scores.[125] And as mentioned above, FICO scores are now used for much more than determining creditworthiness. Score creep, as I call it, is not necessarily a bad phenomenon, but it makes it that much more important to ensure that the score is accurate and accurately used.

B. LAW

Unlike most predictive policing programs, FICO scores fall under the purview of laws that specifically govern it. The Fair Credit Reporting Act (FCRA) governs access to and maintenance of the information in a credit report.[126] The FCRA provides protections to consumers, including the right to know if a credit report is used in adverse actions, the right to see the credit report (except for credit score), and the right to dispute inaccurate information and have that information corrected.[127] If a consumer disputes information with a creditor, the creditor may not report that information without informing the credit bureau of the dispute. Outdated information, which is generally more than seven years

[122] Ibid., 293.

[123] Ibid.

[124] Ibid., 296.

[125] Arya, Eckel and Wichman, "Anatomy of the Credit Score," 175.

[126] 15 U.S.C. §§ 1681–1681u.

[127] Ibid.; see also Avery et al., "An Overview of Consumer Data and Credit Reporting," *Federal Reserve Bulletin*, 48 (February 2003).

old, must be excluded from a credit report.[128] The FCRA prohibits anyone other than those with a permissible purpose to receive a credit report, and a consumer must give written consent to the release of reports to employers or if it includes medical information.[129] A consumer may also opt to exclude himself or herself from receiving unsolicited firm offers of credit or insurance.[130] These protections have proven crucial to ensure that FICO scores are reliable and do not unfairly hinder a person's ability to receive credit (among the many other uses caused by score creep).

Despite this extensive statutory scheme designed to make the FICO score more reliable, flaws exist that are the subject of proposed legislation.[131] The legislation is proposed in light of the fact that credit reporting is the number one complaint to the Consumer Financial Protection Bureau. The complaints range from the cumbersome appeals process for correcting inaccurate data to the fact that the consumer bears the burden to prove the inaccuracy rather than the credit bureau bearing the burden to prove the accuracy.[132] The bill would restrict score creep by limiting how employers can use a credit score in their hiring practices. Additionally, the bill would add more protections to ensure the accuracy of the data, such as removing all paid or settled debts within 45 days of settlement, and requiring notification to the consumer the first time a creditor reports negative information. Additionally, the bill would allow major lenders to rely on more advanced credit scores other than the FICO.[133] For example, VantageScore 3.0 minimizes the effect of medical bills, and other scores include rental information to

[128] Avery et al., "An Overview of Consumer Data and Credit Reporting." There are exceptions, such as that criminal convictions have no time limits, bankruptcy information for 10 years, information reported in response to an application for a job with an annual salary of more than 75,000 has no time limit nor does an application more than $150,000 worth of credit or life insurance information about a lawsuit, unpaid judgment, or record of arrest can be reported for seven years or until the statute of limitations runs out, whichever is longer.

[129] Ibid.

[130] Ibid.

[131] Kenneth R. Harney, "Bill Attempts to Protect People from Flaws in Credit-Reporting System," *Washington Post*, June 1, 2016, https://www.washingtonpost.com/realestate/bill-attempts-to-protect-people-from-flaws-in-credit-reporting-system/2016/05/31/40186c48-2743-11e6-ae4a-3cdd5fe74204_story.html.

[132] Ibid.

[133] Ibid.

permit non-homeowners to build better credit.[134] These differences highlight the issues created by the fact that FICO has not been updated in over decade,[135] and show that all predictive analytic programs must be continually updated to adapt to the current societal trends.

C. VARIETY AND VOLUME OF DATA

The FCRA prohibits entities from knowingly providing inaccurate information to the credit bureaus or from consciously avoiding knowledge that the information is inaccurate. Additionally, these entities must participate in the correction of inaccurate data. Although each credit bureau collects slightly different information, the information that is included in a credit report generally includes five types of information:[136]

- Basic identification information such as name, residential address, date of birth, and Social Security number.
- Information from creditors on loans, leases, and other such bills.
- Information from public records that pertain to finances, such as bankruptcies and foreclosures.
- Information from collection agencies.
- Information about individuals or entities that request information from an individual's credit report.

Although this is a vast amount of information, credit reports are neither comprehensive nor complete pictures of the consumer's' financial life.[137] Some credit accounts may not be included; for example, smaller financial companies and some government agencies may not report to credit bureaus.[138] Additionally, some loans may not be included, such as loans from individuals, employers, and foreign entities. Lastly, creditors may not quickly inform credit bureaus of changes in accounts, especially closed accounts. Creditors, government entities, collection agencies, and other various third-

[134] Ibid.

[135] Ibid.

[136] Avery et al., "An Overview of Consumer Data," 48.

[137] Ibid., 50.

[138] Ibid.

party intermediaries voluntarily provide all of the information to the credit bureau.[139] The bureaus collect information every month and update their records within one to seven days.[140] Hence, there is a lag in the data reported.

D. VERACITY OF DATA

One would assume with the due process protections provided by the FCRA and the variety and volume of data relied upon to create the FICO score that it would be easy to fulfill the veracity aspect of predictive analytics. However, the data is sometimes wrong. After all, the credit bureaus have the incredibly difficult job of producing accurate credit reports for *everyone*. A simple typo in a name or a Social Security number, or a consumer's name change can lead to the addition of information to the wrong credit report.[141] It is the basic difficulty of any database that is based on biographical information as opposed to biometrics.

FICO still receives its information from the three major American credit bureaus, which maintain credit histories on over two hundred million consumers.[142] The data reported to credit bureaus on consumers comes from more than 30,000 entities.[143] From this data, the bureaus process about "two billion individual account updates, two million new public record items, and 3.3 million changes of address monthly."[144]

Credit bureaus review information they receive for accuracy before including it in an individual's report.[145] If the information is found to be inaccurate, the credit bureaus returns it to the entity for correction and resubmission. Besides checking for accuracy, the credit bureaus must then determine "when to ignore slight variations in personal identifying information and … recognize [when] data items with the same identifying

[139] Ibid.

[140] Ibid., 49.

[141] Ibid., 53.

[142] Ibid.

[143] Ibid.

[144] Smith et al., "Accuracy of Information Maintained," 589.

[145] Avery et al. "An Overview of Consumer Data," 49.

information, such as name, may actually be associated with different individuals."[146] Thus, ensuring that the data is accurate is extremely difficult. Even with all of the various steps, credit rating bureaus still hold inaccurate data that can affect an individual's FICO score.

Therefore, it is not surprising that with that much data to handle and update, the information—and consequently, the score—is not 100% correct. Furthermore, many of the problems occur when third parties report incorrect information to the credit bureaus. Fixing the inaccurate data held by third- and fourth-party providers is out of the control of FICO and the credit bureaus.

Despite these significant issues, the FICO score can, for the majority of consumers, predict who within the United States is more likely to repay debts. But for some consumers, the data errors within the U.S. credit bureaus can cause significant problems. Smith et al. conducted a study that shows the number of individuals who are impacted by an inaccurate FICO score. In their study, they sampled 1,000 American consumers and reviewed their credit reports from the three bureaus. Out of those studied, 26% found at least one material error.[147] An interesting aspect of their study is that they also followed those individuals as they attempted to correct the errors. Only 78% of those individuals were able to have at least one bureau alter the information in their credit rating.[148] This alteration often made significant differences to the credit scores. Their conclusion was that credit scores can be a good indicator of creditworthiness, but only if consumers are vigilant to ensure that the data included in their score is accurate.[149] Despite the need for vigilance, only about 38% of consumers annually verify their information held by the credit bureaus.[150] Placing the onus on consumers to ensure the

[146] Ibid., 50.

[147] Smith et al., "Accuracy of Information Maintained," 593.

[148] Ibid., 594, 600, noting that because consumers had the assistance of the researchers in filing their disputes, the participants in this study may have had more success than a normal consumer.

[149] Ibid., 600.

[150] Ibid., 599. You can (and should) check your own report at www.annualcreditreport.com. Anecdotally, when I finally did check my credit report, thanks to this thesis, one of the credit bureaus thought I was married to my father. Luckily, it was an easy fix for me.

accuracy of the data saves significant resources for the bureaus, but it does not ensure the accuracy of the data. Furthermore, it pushes the economic cost onto the consumers because the consumers pay higher fees due to the incorrect information.[151]

[151] Poon, "Scorecards as Devices," 296

VI. SECURE FLIGHT: WHY YOUR FRIEND ALWAYS GETS PRECHECK FOR FREE

The Transportation Security Administration (TSA) within the Department of Homeland Security created Secure Flight in 2009. At first, the only goal was to identify airline passengers who posed a high risk by matching those individuals against federal government watch lists.[152] In 2011, the program expanded to include lists of pre-approved low-risk travelers, such as those in the TSA Precheck program. This eventually evolved, and now Secure Flight conducts risk analysis for individuals on a per-flight basis to determine their general risk to aviation security.[153]

It is possible for citizens to know the type of the information used by Secure Flight, unlike several state and local predictive policing programs. The Privacy Act of 1974, as mentioned previously, requires the federal government to maintain a System of Records Notice (SORN) for most databases of this type.[154] Secure Flight collects data from aviation passengers as well as others who enter the secured areas of airports.[155] The data collected is then used to assess the risk of the passenger on a per-flight basis. If an individual matches a watch list, he or she will receive enhanced screening and may be prohibited from flying. For all other individuals, the program, through an algorithm, conducts a risk-based analysis of the data collected to determine whether the individual is a low or moderate risk.[156] If the individual is considered a low-risk passenger, then the individual is routed to the TSA Precheck line.[157] The individuals considered a moderate risk use the standard line. Although the Secure Flight risk assessment also is capable of determining if an individual is a high risk, the Secure Flight risk assessment is not used to

[152] GAO, *TSA Has Taken Steps to Improve Oversight of Key Program*, 3.

[153] Ibid., 4.

[154] 5 U.S.C. § 552a (a)(5); see also OMB Guidelines, 40 Fed. Reg. 28,948, 28,952 (July 9, 1975).

[155] DHS/TSA-019 Secure Flight Records System of Records, 233, 238.

[156] Ian David Fiske, "Failing to Secure the Skies: Why America Has Struggled to Protect Itself and How It Can Change," *Virginia Journal of Law& Technology* 15 (2010): 173, 186.

[157] Government Accountability Office (GAO), *TSA Should Take Additional Steps to Determine Program Effectiveness* (GAO-14-531) (Washington, DC: GAO, 2014), 26–34.

forbid an individual from flying or entering the secure area of an airport. Secure Flight only denies an individual the ability to fly if the individual's name matches to a name on the No Fly List.[158]

The data used in Secure Flight comes from several databases, including the Computer-Assisted Passenger Prescreening System (CAPPS), which assesses passenger name records (PNR), and other information contained in flight reservations collected by aircraft operators such as

- the No Fly List;
- the Terrorist Screening Database (TSDB);
- lists of low-risk individuals, such as TSA Precheck known travelers;
- frequent flyer designator codes; and
- other classified and unclassified governmental law enforcement, immigration, or intelligence databases.[159]

The TSA is also considering the use of commercial databases to verify the information provided by airline passengers.[160] Data that is not associated with a match to a watch list is destroyed within seven days of the flight and is only kept if a passenger complains that he or she was wrongly identified under the system.[161]

One of the main criticisms against Secure Flight is the lack of performance measures to ensure that the program is meeting its goals.[162] TSA collects information about the number of individuals matched as high or low risk, but it does not keep metrics on the extent of matching errors—either false negatives or false positives.[163] As of April 2014, TSA was still developing appropriate metrics to determine this crucial performance metric.[164] Additionally, as with most predictive analytics programs, there is concern that

[158] Ibid.

[159] DHS/TSA-019 Secure Flight Records System of Records, 233, 236.

[160] Fiske, *Failing to Secure the Skies,* 173, 186.

[161]DHS/TSA-019 Secure Flight Records System of Records, 233, 236.

[162] GAO, *TSA Should Take Additional Steps,* 26–34.

[163] Ibid.

[164] Ibid.

due process is not adequately protected by Secure Flight, given that many of the databases it relies on cannot be checked for accuracy by average citizens.[165]

[165] James Fisher, "What Price Does Society Have to Pay for Security? A Look at the Aviation Watch Lists," *Willamette Law Review* 44 (2008): 573, 580, noting that the TSDB and No Fly Lists cannot be reviewed by citizens.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. ANALYSIS: OR THE POINT OF THIS THESIS

At this point, you may be thinking: So what? Clearly, these are three perfectly legitimate and legal uses of predictive analytics. All three greatly help society: FICO prevents financial ruin, Secure Flight helps keep the TSA lines shorter and moving faster, and predictive policing helps manage law enforcement resources. The key here is to learn from the mistakes of these existing programs to improve the planning of new ones. FICO, despite being around for a few decades, still has some significant problems, as does Secure Flight. Before law enforcement widely begins using predictive policing programs to predict what humans might do, the agencies and departments should learn from these predictive analytics pitfalls and adjust their programs accordingly. So often, a new tool or technology is put into use without fully understanding the bad that comes with the good. The lack of understanding can lead to misuse, and misuse can undermine the tool's benefits. This leads to the tool being severely hampered by overly corrective policies or being taken away altogether.

How does a program avoid the aforementioned pitfalls and their likely consequences during the establishment of a predictive analytics program? One way is to use the Five Vs as a framework to evaluate the effectiveness of the predictive policing program. Each program will have strengths and weaknesses when assessed against the Five Vs, and by using those elements, predictive policing programs can make an assessment of the program. For the purpose of this thesis, it proves useful to compare and contrast FICO, Secure Flight, and predictive policing through the Five Vs Framework.

A. THE FIVE VS

1. Volume

As mentioned earlier, the brilliance of big data is that scientists and analysts do not need to rely on a small amount of data in order to form a prediction. Long gone are the days of creating a sample set of data, similar to the FICO scorecards. Rather, big data allows for all data within a dataset to be used and all individuals to be compared to each

other. This creates a better baseline to know what is normal behavior to then better detect abnormal behavior.

FICO keeps a credit score for every individual who has some form of credit. Even individuals who have never had any form of credit have a score—it is just incredibly low. This baseline makes anomalies much easier to detect because everyone who has or needs credit is compared against each other. Additionally, FICO can come fairly close to collecting all datasets on individuals that may determine whether they will pay their debts because FICO focuses only on creditworthiness. However, because FICO and the credit bureaus must rely on third parties to accurately and timely report the data, the volume needed for an accurate assessment may be incorrect, as is the case if the data is late or inaccurate, or if a third party never provides the data.

Secure Flight attempts to assess individuals as either low or moderate risk in terms of potential for sabotaging air flight. That seems like a narrow focus; however, there are various datasets that could apply to this determination because there is not an exact profile of people who want to sabotage planes. Therefore, the fact that Secure Flight mostly limits its datasets to information that is directly related to airline flights may be an overly narrow scope for the objective. Additionally, Secure Flight deletes the determination and data shortly after the flight finishes. So even though Secure Flight collects information on all airline passengers, the lack of a clear profile of terrorists and the lack of historical data means that Secure Flight may not have the volume of data needed to make an accurate risk assessment. Consequently, Secure Flight may not have the correct baseline of data for the algorithm to determine the normal as opposed to the abnormal.

Most predictive policing programs will face similar problems to those experienced by Secure Flight because of the inability to determine a proper baseline. A multitude of factors can foster an atmosphere that will lead an individual to commit crime. The question of who within a society will commit a crime is not a narrow question. The predictive program, in order to answer that question, will need to use several datasets, depending on which theory of criminology the programmer opts to follow. At this point, it is difficult to fully analyze whether predictive programs achieve

volume because most of the programs do not release this information. It is considered the proprietary information of the private companies that create the programs.[166]

However, it is doubtful that any of the predictive policing programs collected information on every citizen within its jurisdiction. As uncomfortable as this is to admit, in order to create a baseline that effectively determines who is likely to commit a crime, programs need to collect information from the whole of the community, much like FICO. Arguably, the predictive programs that predict which parolees will be recidivists may come closest to a complete baseline. Here, being able to use all datasets of all parolees creates a solid baseline because the question to be answered is narrow: Which parolees will be recidivists? The question is not asking which citizens will be recidivists. Because predictive policing programs that seek to predict who will be involved in crime ask such broad questions, the programs need a broad baseline and a large volume of information.

We, as a society, must determine if the accuracy of a predictive policing program is worth the potential tradeoff in privacy. A better baseline will ensure a better risk assessment but will require police departments to collect a significant amount of information on all citizens. China determined this issue by choosing the more accurate baseline over privacy. China directed its largest state-run defense contractor, China Electronic Technology Group, to create a program that is capable of assessing each citizen's likelihood of being a terrorist.[167] This "united information environment," as China calls it, will collect data on jobs, hobbies, consumption habits, and other various data streams.[168] This combined with a proposed law that would grant the Chinese

[166] Pennsylvania Commission on Sentencing, *Risk Assessment Project II, Interim Report 2, Validation of Risk Assessment Instrument by Offense Gravity Score for All Offenders*, Feb. 2016, http://pcs.la.psu.edu/publications-and-research/research-and-evaluation-reports/risk-assessment. Pennsylvania is one of the few states that *does* release information on its predictive policing program because the state, not a private company, built the program itself. All of the Pennsylvania Commission on Sentencing reports are available to the public.

[167] Shai Oster, "China Tries Its Hand at Pre-Crime," *Bloomberg Businessweek*, March 3, 2016 http://www.bloomberg.com/news/articles/2016-03-03/china-tries-its-hand-at-pre-crime; for further discussion, see also Cara McGoogan, "'Minority Report'—Style Technology to Predict Crime in China," *Telegraph*, March 8, 2016, http://www.telegraph.co.uk/technology/2016/03/09/minority-report-style-technology-to-predict-crime-in-china/.

[168] Oster, "China tries Its Hand."

government vast access to user data for national security purposes would allow China to have a baseline similar to FICO's baseline for predictive policing purposes.

2. Variety

Variety is ensuring that data comes from various sources, which creates a stronger baseline for the algorithm to make its prediction. Finding the right balance of sources will always be difficult because the more variety, the more likely that the information may be inaccurate. Additionally, in order to have variety, the analytic program must persuade a third party to hand over its data. Even though there are statutes that encourage entities to voluntarily give data to the credit bureaus, FICO still has difficulty gathering the financial data from these various sources. Secure Flight also has difficulty with variety because a significant portion of the data that Secure Flight relies on is data created and maintained by the government. It can be assumed that predictive policing programs will also have difficulty with variety.[169]

Variety is critical for predictive analytics because it helps to ensure accuracy of the data. Additionally, as a predictive analytic assessment is used for more than its original use, such as how FICO is used for much more than just creditworthiness, this score creep will require a larger variety of data. FICO scores are used to help determine if a person should receive a job, is date worthy, is trustworthy, and so on. The score creep phenomenon is also affecting some of the data used by Secure Flight because of legislation to deny firearms to those who are on the No Fly List.[170] Any predictive policing program must assume that its risk analysis will eventually be used for more than just determining who may be involved in crime.

---

[169] I admit that this is an assumption on my part, because very little is released about the data used by predictive policing programs due to their proprietary nature. To delve into the problem of having private entities create significant technological programs for government would take another thesis, but suffice it to say that the utter lack of transparency of most of these programs is disturbing, especially given the significant governmental decisions that the programs are making about people. For more on this issue, see Greg Ridgeway, "The Pitfalls of Prediction," *National Institute of Justice Journal* 271 (February 2013), which identified a lack of transparency as one of the seven pitfalls for predictive policing programs; and Uchida, *A National Discussion on Predictive Policing*, which noted the need for transparency.

[170] David M. Herszenhorn, "Bipartisan Senate Group Proposes 'No Fly, No Buy' Gun Measure," *New York Times*, June 21, 2016.

Currently, there is not much one can do to prohibit score creep. Nothing in the laws or regulations forbids individuals from basing decisions off of these predictive risk assessments. This is especially troubling when one considers that the predictive analytics program often only collects data to answer a specific question. Thus, if a program does not include enough variety of data to accurately answer the initial question, when score creep occurs the prediction will be that much more inaccurate. Because people often assume that any assessment that comes from a computer is absolutely accurate, score creep must be considered when creating a predictive analytics program. Without the proper understanding of the exact predictive question that the algorithm is answering, the datasets included, and the acceptable predictive probability, people will use the predictive assessment incorrectly.

3. Velocity

Not surprisingly, I do not have access to the data processing speeds of FICO, Secure Flight, or Predictive Policing programs. Velocity is key because if the data is not up to date, even up to the minute, then the algorithm will be inaccurate. In other words, the more stale the data, the more stale the prediction.

The credit bureaus have problems with keeping up-to-date data because reporting entities often do not report information in a timely way. This lag time can sometimes help consumers, and it can sometimes hurt consumers. Either way, the lag time hurts FICO's accuracy.

Secure Flight is unique because it draws from several protected datasets as well as the databases from private entities (airlines). One of the protected datasets is the No Fly List. The process to add a name to the No Fly List is complicated, which creates significant lag time. First, the individual must be nominated to the Terrorist Screening Database. Then, the Terrorist Screening Center must accept the nomination. If an

individual fits certain criteria, he or she is nominated for the No Fly List. TSA then reviews and either accepts or rejects the nomination.[171]

This process takes time, and depending on your point of view, that can be good or bad. It is bad if you want the most up-to-date predictive analytics program because the faster the information is included in the algorithm, the faster the computer can learn from the data and make necessary adjustments. At the same time, we cannot forget that the Terrorist Screening Database and the No Fly List have significant impacts on individuals' lives. Before limiting an individual's fundamental right to travel or intimating to the law enforcement community that someone may be a terrorist, there should be a well-established and thorough process. Even if Secure Flight's risk assessment is done by a computer, the choice to include someone in several of the databases that feed into Secure Flight is a human one, and human decisions are fraught with errors. Consequently, a key for predictive policing programs will be to find the balance between maintaining up-to-date data and ensuring that the data is accurate before it is added to the database.

4. Veracity

The errors caused by human decisions play directly into the veracity of the data used by predictive analytic programs. In order for a predictive analytics program to make accurate predictions, it needs accurate data. Veracity will always be one of the hardest of the Vs for any program to achieve. Sometimes, data is incorrectly inputted; other times, a person makes an incorrect assumption. Sometimes, data becomes inaccurate with time.

For a large database, FICO does fairly well ensuring the accuracy of its data, but, as was mentioned previously, it still has problems significant enough to warrant proposed legislation to fix inaccuracies. This is troubling for predictive policing programs—that even a thoroughly transparent predictive analytic program like FICO still experiences significant problems with accurate data. Several scholars have called for transparency in

[171] Sharon Bradford Franklin and Sarah Holcomb, "Watching the Watch Lists: Maintaining Security and Liberty in America," *Human Rights* 34 (207): 18, 19; see also Ibrahim v. Dept. of Homeland Security, 62 F. Supp. 3d 909, 931(D. N. Ca. 2014), noting that an FBI agent incorrectly check the box to nominate Ibrahim to the No Fly List.

the creation of predictive policing programs,[172] but as the inaccuracy issue with FICO shows, transparency is not the only answer. A well-defined and effective process to correct that data is also necessary. Remember, only 78% of individuals with inaccurate data are able to have at least one bureau alter the information in their credit rating.[173] Creating and maintaining this process is where most predictive analytic programs fail.

Although the Government Accountability Office admonished Secure Flight to improve the accuracy of the data it uses, Secure Flight, like FICO, has had difficulties with this.[174] Transparency with the public is difficult because Secure Flight relies on several databases that are not open to public review and critique. Many of these databases, like the No Fly List and the Terrorist Screening Database, contain information collected for and used in ongoing law enforcement investigations. To allow the public to review that data for accuracy would compromise the investigations. The same will hold true for some of the data included in predictive policing programs. This creates an enormous challenge: the need to balance the secrecy of ongoing investigations with an individual's need and potential due process right to correct inaccurate information about them.

The No Fly List, which feeds into Secure Flight, shows that Secure Flight, like FICO, also fails in creating an effective process to correct data. The courts determined that the DHS Traveler Redress Inquiry Program (DHS TRIP) did not meet the requirements of due process, and as a result, the courts required DHS to revamp the program.[175] In other words, DHS has not created an effective process to allow people to correct inaccurate data that the No Fly List maintains about them.

---

[172] See, for example, Uchida, *A National Discussion on Predictive Policing*; Ridgeway, "The Pitfalls of Prediction," noting that one of the seven pitfalls of predictive policing is not focusing on transparency.

[173] Smith et al., "Accuracy of Information Maintained by U.S. Credit Bureaus: Frequency of Errors and Effects on Consumers' Credit Scores," *The Journal of Consumer Affairs* (Fall 2013): 594, and 600.

[174] Government Accountability Office, *Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed* (GAO-05-356) (Washington, DC, GAO, March 2005), 3.

[175] Latif v. Holder, 28 F. Supp 3d 1134, 1161–62 (D. Or. 2014), finding the TSA redress procedures did not meet the constitutional for due process; Ibrahim v. Dept. of Homeland Security, 62 F. Supp. 3d 909, 931(D. N. Ca. 2014), finding that TSA did not provide constitutional due process to plaintiff.

The difficulty of ensuring the veracity of data highlights three significant issues with predictive analytics programs. First, governmental and private entities are making significant decisions about individuals, but those decisions are largely unreviewable. With predictive policing, a police department determines who is likely to be involved in a crime or a recidivist, yet those individuals have little redress to challenge those decisions. Second, the third- or fourth-party datasets that feed into these programs need review. The No Fly List is not part of the Secure Flight program, but the data from the No Fly List is used by the algorithm that determines an individual's risk score. Thus, the redress concerns for inaccurate data may flow beyond the initial predictive program. Finally, not all datasets that feed into the predictive program will be governed by the same laws. FICO is not a government entity; therefore, the Fourth Amendment does not apply. State and local law enforcement groups do not need to abide by the Privacy Act, nor do private entities that collect a large portion of the data now available. If predictive policing programs rely on data from private entities that are not regulated, then significant governmental decisions are being made based on unregulated data.

5. Verification

Verification, simply put, is testing the predictive analytics program. Without verification, the end user—whether governmental or private entities—cannot be sure that the forecast made by the predictive analytics program is accurate. Verification requires metrics. Without finding the right metrics to measure the predictive analytics program, the program runs the risk of making inaccurate predictions.[176] The metrics ensure that the natural biases of the programmer do not create inaccurate forecasts by either emphasizing or deemphasizing certain datasets.[177] Additionally, the metrics help the programmer know if the data that is being relied upon is accurate. Furthermore, predictive analytics are algorithms that need to "learn from their own mistakes" (formally known as machine learning). However, if a program is never told when it gets a prediction wrong, the program cannot learn and correct itself. Metrics are also required in order to set an

[176] Siegel, *Predictive Analytics*, 79.

[177] Sweeney, *Discrimination in Online Ad Delivery*; for further discussion, see Gillespie, "The Relevance of Algorithms."

acceptable rate of false negatives and false positives. No matter how accurate the algorithm or the data every predictive analytic program will make a wrong prediction because humans do not always follow the norms.[178] However, without accurate metrics, the programmer cannot determine the percentage of false positives and negatives and cannot adjust the algorithm accordingly.

It is easier to measure some predictive analytic programs than others. FICO, for example, is one of the easier programs to verify because once someone receives a credit score, either they act according to that score or they do not. So, assuming the FICO scores are accurate, someone who has a low score will not repay their loans as often as someone who has a high score. If the prediction does not occur, the algorithm can analyze the wrong predictions and make adjustments as necessary. Secure Flight is an example of a predictive analytics program that is difficult to measure. Secure Flight determines who is a low-risk passenger, and then he or she can go through the Precheck line instead of the normal security line. In one sense, Secure Flight can measure its accuracy because no one has gone through the Precheck line that intended to bring dangerous items on the airplane. But just because something has not occurred, does not mean Secure Flight's assessments have been verified. There are probably a number of people who were sent to the normal security line who should have gone to the Precheck line. In order to know if Secure Flight assessments are correct, the program must prove a negative, which is extremely difficult to do.[179]

Predictive policing programs will find themselves in much the same predicament as Secure Flight. It will be extremely difficult for Chicago to know if one of the 400 people on its heat list will never be involved in a violent crime because that would require actually predicting the future.[180] A parole board that chooses to deny someone parole will never know if that individual would have been a recidivist if released from jail. Consequently, police departments need to recognize that a crucial element of predictive

[178] Siegel, *Predictive Analytics*, 79.

[179] Ibid.

[180] Chicago could follow the individuals until they die. However, that would be an extremely long study with severe implications on civil rights, civil liberties and privacy of the innocent individuals.

analytics—machine learning—will not occur in many predictive policing programs without viable metrics. Without machine learning, the algorithm will not be able to adjust to changing crime trends. With no ability to verify the predictions, there is no way to know whether the people the departments target are actually bad guys or just victims of police harassment

Only relying on a drop in crime rate does not verify that the predictive analytics made a correct forecast. Take, for example, the Greater Manchester Police's pilot program using predictive policing. The burglary rate dropped by 26.6% during the period of review. However, during this period, the police assisted in "hardening" 250 properties, and contacted 416 property owners face-to-face.[181] The Manchester Police relied on the forecast to determine which properties to harden, which arguably saves police and community resources, but any property that is hardened is less likely to be burgled. Thus, the decrease in burglary rate may have only been caused by the increase in police activity.

Furthermore, the pilot only focused on the Greater Manchester area. Therefore, while the burglary rates for that area did decrease, the burglary rates for the adjacent area may have increased.[182] In a sense, by making a forecast and focusing police resources the predictive analytics program may then become wrong. It is like a kind of "Butterfly Effect."[183] As soon as the prediction is acted upon and the police refocus their resources, the criminals do, as well. This is why good metrics to feed into machine learning is incredibly important for predictive policing programs. At this point in predictive analytics, there is not an analytic program with fast enough machine learning to handle these quick and subtle shifts. Because just as law enforcement is being revolutionized by technology, so is crime.[184]

The recent study of the Chicago Police Department's predictive policing program also shows that only relying on crime rate is not enough. The report, which studied the

[181] Newbold, " 'Predictive Policing,' 'Preventative Policing,'"13.

[182] Newbold, " 'Predictive Policing,' 'Preventative Policing,'" 13.

[183] Ibid.

[184] Newbold, " 'Predictive Policing,' 'Preventative Policing,'" 28.

data from 2013, showed that an individual on the list was not more or less likely to be involved in homicide than the comparative group, but an individual on the list was more likely to be arrested.[185] The report proposed that the higher arrest rate could be because police officer used the list as leads, but notes that the higher arrest rate does raise significant "privacy and civil rights considerations that must be carefully considered, especially for predictions that are targeted at vulnerable groups at high risk of victimization."[186] Therefore, predictive policing programs must work to find viable metrics to continually verify that the predictive policing program has kept up with the crime trends.

[185] Saunders, Hunt, and Hollywood, "Predictions Put into Practice," 1–25.

[186] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. CONCLUSION

The most obvious, yet most likely forgotten, approach to the challenges facing predictive policing programs is to understand that using predictive analytics to predict human behavior is a relatively new technology that still has bugs in it. These programs need to train police officers fully on the limitations of the predictions. The training should include an understanding of the data relied upon, and the number of false negatives and false positives that the system tends to forecast. Without this thorough understanding, police officers will easily misuse the forecast.

A. SELF-POLICING

The first step in ensuring a reliable program is to thoroughly vet the data. Even though there are proprietary concerns because most of the programs are created by the private sector, the law enforcement department needs full knowledge of the datasets being used and which third or fourth parties provided the data. Even if full transparency cannot be given to the public because of proprietary concerns or law enforcement concerns, the department must have full transparency into how the predictive policing program was created and is maintained.

Not only must the program ensure that the data is accurate but the predictive policing programs must set up viable redress programs as soon as the program is put in place. The programs will not be able to provide transparency due to law enforcement sensitive information, but having a viable and robust redress program will demonstrate to the public that the program can still be trusted. Additionally, the redress programs will make the assessments stronger. If there is incorrect data, it needs to be corrected so that police resources are not wasted targeting the wrong people.

The police department must also create clear metrics to measure the system. Currently, the main metric used to measure if a predictive policing program works is a reduction in crime rate, but, as mentioned earlier, this may not be an accurate metric. Rather, I think A/B Testing would be more beneficial. A/B Testing is often used to test

which version of an app or website is better liked by potential clients.[187] Both versions are launched, data is collected, and by comparing the data, determinations can be made about which version was more productive. For predictive policing, it can be done by using predictive policing in comparing groups of people, similar to the Saunders study in the *Journal in Experimental Criminology*. The data is then collected, and the various areas can be compared to one another. Therefore, the status quo is measured against the predictive policing effects. If the predictive policing remains the same to the status quo, then predictive policing has not added anything. Tests would need to be tailored to each jurisdiction, but it seems to be the only way to find a true metric that could possibly prove the negative because at least with A/B Testing, the program will be accurately measured against the status quo. Additionally, the recently released study on Chicago's predictive policing program shows promise for finding viable metrics. The Saunders study used two-quasi experimental methods—an interrupted time-series analysis and propensity score analysis.[188] The study shows that using the two methods in combination gives a fair overview to the effect that the predictive policing program actually had on a given jurisdiction.

B. LEGAL MATTERS

Besides self-policing, there can be some changes in laws that will help the accuracy of predictive policing programs. Predictive policing programs are just one more technology advancement that shows that the Privacy Act of 1974 needs to be amended to

[187] "A/B Testing," IBM, accessed Aug. 31, 2016 https://www.ibm.com/devops/method/content/learn/practice_a_b_testing/.

[188] Saunders, Hunt, and Hollywood, "Predictions Put into Practice," 1–25.

better fit today's technology.[189] One basic requirement should be that the Privacy Act be extended to cover states and private entities in their collection of data. As databases become interoperable and more integrated, the imaginary line between private, federal, and state and local data collections will disappear. In order to have any hope of personal data being protected, the protections must extend to any entity that may collect data.

By thoughtfully researching, creating, and implementing a predictive policing program, police departments could harness an extremely powerful tool to better allocate resources and keep the streets safer. However, if departments do not fully understand the programs they implement, then these programs could waste police resources and make the streets less safe. As such, a police department must ensure that the predictive policing algorithm used relies on the proper volume and variety of data, and is updated in a timely a fashion (velocity). Furthermore, the department must ensure that the data that the algorithm relies on stays accurate (veracity). Finally, the police department must continually test the veracity of the risk assessments made by the predictive policing programs to ensure the risk assessments are accurate.

[189] There are several theories on how the Privacy Act of 1974 should be updated. Although interesting, a thorough discussion is not necessary for this thesis. For further discussion, please see, for example, James McCain, "Apply the Privacy Act of 1974 to Data Brokers Contracting with the Government," *Public Contract Law Journal* 35 (Summer 2009), 935, arguing that a broad reading of 5 U.S. Code § 552a(m) will better protect privacy; Haeji Hong, "Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao," *Akron Law. Review* 38 (2005): 71, suggesting legislative changes to strengthen the enforcement aspects of the Privacy Act of 1974; Robert Gellman, "A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board," *Hastings Law Journal* 54 (April, 2003): 1183, arguing that a privacy agency needs to be created in order to promote best practices; and Joshua D. Blackman, "A Proposal for Federal Legislation Protecting Information Privacy Across the Private Sector," *Santa Clara Computer & High Tech. Law Journal* 9 (Nov. 1993): 431, arguing that there should be federal legislation that requires an individual's authorization prior to disclosing or using personal data.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Arya, Shweta, Catherine Eckel, and Colin Wichman, "Anatomy of the Credit Score." *Journal of Economic Behavior & Organization* 95 (2013): 175–185.

Avery, Robert B., Paul S. Calem, Glenn B. Canner, and Raphael W. Bostic. "An Overview of Consumer Data and Credit Reporting." *Federal Reserve Bulletin*, 48 (February 2003).

Berk, Richard, and Justin Bleich. "Statistical Procedures for Forecasting Criminal Behavior: A Criminal Assessment." *Criminology & Public Policy* 12, (2013): 513–544.

Bernerth, Jeremy B., Shannon G. Taylor, H. Jack Walker, and Daniel S. Whitman. "An Empirical Investigation of Dispositional Antecedents and Performance-Related Outcomes of Credit Scores." *Journal of Applied Psychology* 97(2012): 469–478.

Chan, Janet, and Lyria Bennett Moses, "Is Big Data Challenging Criminology?" *Theoretical Criminology* 20 (2016): 21–39.

Chicago Police Department. "CPD Welcomes the Opportunity to Comment on Recently Published RAND Review." Aug 17, 2016. http://4abpn833c0nr1zvwp7447f2b.wpengine.netdna-cdn.com/wp-content/uploads/2016/08/RAND_Response-1.pdf.

Cisco. "The Zettabyte Era—Trends and Analysis." June 2016. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.

Diakopoulos, Nicholas. *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, Columbia Journalism School, Tow Center for Digital Journalism, Dec. 3, 2014. http://towcenter.org/research/algorithmic-accountability-on-the-investigation-of-black-boxes-2/.

Eligon, John, and Timothy Williams. "Police Program Aims to Pinpoint Those Most Likely to Commit Crimes." *New York Times*, Sept. 25, 2015. http://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html?_r=0.

Federal Register. "Department of Homeland Security Transportation Security Administration - DHS/TSA-019 Secure Flight Records System of Records." Jan. 5, 2015.

Ferguson, Andrew Guthrie. "Big Data and Predictive Reasonable Suspicion." *University of Pennsylvania Law Review* 163 (2015): 327–428.

———. “Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards,” *Oklahoma Law Review* 66 (2014): 831–874.

———. “Predictive Policing and Reasonable Suspicion.” *Emory Law Journal* 62 (2012): 261–325.

Fisher, James. “What Price Does Society Have to Pay For Security? A Look at the Aviation Watch Lists,” *Willamette Law Review* 44 (2008): 573–613.

Fiske, Ian David. “Failing to Secure the Skies: Why America Has Struggled to Protect Itself and How It Can Change,” *Virginia Journal of Law& Technology* 15 (2010): 173–197.

Franklin, Sharon Bradford, and Sarah Holcomb, “Watching the Watch Lists: Maintaining Security and Liberty in America.” *Human Rights* 34 (2007).

Gardner, Andrea. “Can an Algorithm Predict Child Abuse? L.A. County Child Welfare Officials Are Trying to Find Out.” Southern California Public Radio, Jan. 13, 2015. http://www.scpr.org/news/2015/01/13/49191/can-an-algorithm-predict-child-abuse-la-county-chi/.

Gillespie, Tarleton. “The Relevance of Algorithms.” In *Media Technologies: Essays on Communication, Materiality, and Society*, edited by Tarleton Gillespie, Pablo Boczkowski, and Kirsten Foot, 167–194. Cambridge, MA: MIT Press, 2014. http://mixedrealitycity.org/readings/Gillespie_TheRelevanceofAlgorithms.pdf.

Government Accountability Office (GAO). *Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed* (GAO-05-356). Washington, DC, GAO, March 2005.

———. *TSA Has Taken Steps to Improve Oversight of Key Program, but Additional Actions Are Needed* (GAO-15-559T). Washington, DC: GAO, May 13, 2015.

Harney, Kenneth R. “Bill Attempts to Protect People from Flaws in Credit-Reporting System.” *Washington Post*, June 1, 2016. https://www.washingtonpost.com/realestate/bill-attempts-to-protect-people-from-flaws-in-credit-reporting-system/2016/05/31/40186c48-2743-11e6-ae4a-3cdd5fe74204_story.html.

Herszenhorn, David M. “Bipartisan Senate Group Proposes ‘No Fly, No Buy’ Gun Measure,” *New York Times*, June 21, 2016. http://www.nytimes.com/2016/06/22/us/politics/senate-gun-control-no-fly-list-terrorism.html?_r=0.

IBM. “A/B Testing.” Accessed Aug. 31, 2016. https://www.ibm.com/devops/method/content/learn/practice_a_b_testing/.

IBM Big Data & Analytics Hub. “The Four Vs of Big Data,” Accessed Aug. 12, 2016. http://www.ibmbigdatahub.com/infographic/four-vs-big-data.

International Communication Association. “Preconference Call for Papers: Algorithms, Automation and Politics.” Accessed Aug. 2, 2016. http://www.icahdq.org/conf/2016/AlgorithmsCFP.asp.

Joh, Elizabeth E. “Policing by Numbers: Big Data and the Fourth Amendment,” *Washington Law Review* 89 (2014): 35–68.

Lie, Ying. “Big Data and Predictive Business Analytics.” *Journal of Business Forecasting* (Winter 2014–2015): 40–42.

Loeber, Rolf, Dustin Pardini, D. Lynn Homish, D. L., Evelyn H. Wei, David Farrington, Judith Creemers, Anne Crawford, Magda Stouthamer-Loeber, Steven A. Koehler, and Richard Rosenfeld. “The Prediction of Violence and Homicide in Young Men.” *Journal of Consulting and Clinical Psychology* 73 (2005):1074–88. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.483.6423&rep=rep1&type=pdf.

Madrigal, Alexis. “How Much Is Your Data Worth? Mmm, Somewhere between Half a Cent and $1,200.” *Atlantic*, March 19, 2012. http://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/.

McGoogan, Cara. “ ‘Minority Report’—Style Technology to Predict Crime in China.” *Telegraph*. March 8, 2016. http://www.telegraph.co.uk/technology/2016/03/09/minority-report-style-technology-to-predict-crime-in-china/.

Morgan, Jacob. “A Simple Explanation of ‘The Internet of Things,’” *Forbes*, May 13, 2014, http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#15c4d0d16828.

Newbold, Joe. “‘Predictive Policing,’ ‘Preventative Policing’ or ‘Intelligence Led Policing.’ What Is the Future?” Warwick Business School, Coventry, UK, 2015.

Office of Management and Budget, “Memorandum for the Heads of Executive Departments and Their Agencies: Guidance for Providing and Using Administrative Data for Statistical Purposes.” Feb. 14, 2014. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-06.pdf.

Orwell, George. *1984.* New York: Signet Classics, 1949.

Oster, Shai. “China Tries Its Hand at Pre-Crime.” *Bloomberg Businessweek*, March 3, 2016. http://www.bloomberg.com/news/articles/2016-03-03/china-tries-its-hand-at-pre-crime.

Pell, Stephanie K. “Systematic Government Access to Private-Sector Data in the United States.” *International Data Privacy Law* 2 (2012): 245–254.

Pennsylvania Commission on Sentencing, *Risk Assessment Project II, Interim Report 2, Validation of Risk Assessment Instrument by Offense Gravity Score for All Offenders*, Feb. 2016, http://pcs.la.psu.edu/publications-and-research/research-and-evaluation-reports/risk-assessment.

Perry, Walter L, Brian McInnis, Carter C. Price, Susan Smith, and John S. Hollywood. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND, 2013.

Podesta, John, Penny Pritzker, Ernest J. Moniz, John Holdren, and Jeffery Zients. *Big Data: Seizing Opportunities, Preserving Values*. Washington, DC: Executive Office of the President, May 2014.

Poon, Martha. "Scorecards as Devices for Consumer Credit: The Case of Fair, Isaac & Company Incorporated," *Sociological Review* (2007): 284–306.

Rhee, Nissa/ "Study Casts Doubt on Chicago Police's Secretive 'Heat List,'" *Chicago*, Aug. 17, 2016, http://www.chicagomag.com/city-life/August-2016/Chicago-Police-Data/.

Ridgeway, Greg. "The Pitfalls of Prediction," *National Institute of Justice Journal* 271 (February 2013).

Ritter, Nancy. "Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise," *National Institute of Justice Journal*, 271(February 2013), http://www.nij.gov/journals/271/pages/predicting-recidivism.aspx.

Saunders, Jessica, Priscillia Hunt, and John S. Hollywood. "Predictions Put into Practice: A quasi-experimental Evaluation of Chicago's Predictive Policing Pilot." *Journal of Experimental Criminology* 12 (2016): 1–25.

Siegel, Eric. *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, Revised and Updated*. Hoboken, NJ: John Wiley & Sons, 2016.

Smith, L. Douglas, Michael Staten, Thomas Eyssell, Maureen Karig, Beth A. Freeborn, and Andrea Golden. "Accuracy of Information Maintained by U.S. Credit Bureaus: Frequency of Errors and Effects on Consumers' Credit Scores." *The Journal of Consumer Affairs* (Fall 2013): 588–601.

Stewart, Christopher S., and Mark Maremont. "Twitter Bars Intelligence Agencies from Using Analytics Service." *Wall Street Journal*, May 8, 2016. http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682.

Sweeney, Latanya .*Discrimination in Online Ad Delivery*. Cambridge, MA: Harvard University, Jan. 28, 2013. http://ssrn.com/abstract=2208240.

Thomsen, Michael, "Predictive Policing and the Fantasy of Declining Violence in America." *Forbes*, June 30, 2014, http://www.forbes.com/sites/michaelthomsen/2014/06/30/predictive-policing-and-the-fantasy-of-declining-violence-in-america/#353047606931.

Toomey, Patrick, and Brett Max Kaufman. "The Notice Paradox: Secrete Surveillance, Criminal Defendants & the Right to Notice," *Santa Clara Law Review* 54 (2014): 843–900.

Uchida, Craig D. *A National Discussion on Predictive Policing: Defining Our Terms and Mapping Successful Implementation Strategies* (Report No. NCJ 230404). Washington, DC: National Institute of Justice, 2009.

"Willy Wonka-Golden Ticket Super Computer," YouTube video, 1:10, from *Willie Wonka and the Chocolate Factory* (1971), posted by mediaFace, March 16, 2010, https://www.youtube.com/watch?v=-VujGNQpRjQ

Zarksy, Tal Z. "Transparent Predictions." *University of Illinois Law Review* (2013): 1503, 1517–1518.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California