HOT PEOPLE: AUTOMATED PROFILING, PRE-CRIME INVESTIGATION, AND THE FOURTH AMENDMENT

Natasha H. Duarte

A thesis submitted to the faculty at the University of North Carolina at Chapel Hill in partial fulfillment of the requirements for the degree of master's in mass communication in the School of Media and Journalism

Chapel Hill
2016

Approved by:

Cathy Packer

Victoria Ekstrand

Anne Klinefelter

ABSTRACT

Natasha H. Duarte: Hot People: Automated Profiling, Pre-Crime Investigation, and the Fourth Amendment
(Under the direction of Cathy Packer)

This thesis explores the legal and policy implications of tools that use data mining and automation to predict the likelihood that an individual will commit a future crime. It refers to these algorithms as “automated profiles” because, like analog crime profiles such as the drug courier profile, the algorithms rely on facially innocent characteristics as indicators of criminal activity. The first half of this thesis discusses how the Fourth Amendment case law concerning the drug courier profile might apply to automated profiling. The second half discusses various policy concerns raised by law enforcement agencies’ use of automated profiling systems. This thesis concludes by making several recommendations for the police departments that use these systems, the agencies that may regulate them, the computer scientists who develop them, and the judges who will review them.

TABLE OF CONTENTS

CHAPTER 1: HOT PEOPLE

Introduction

Four hundred Chicago residents received surprise visits from the police in 2014.[1] During the visits,[2] the residents were warned of the consequences of engaging in criminal activity.[3] The residents were on a "heat list" of the 400 Chicago residents most likely to commit a violent crime. [4] Heat lists traditionally consist of individuals with outstanding warrants, but this list was different—some individuals on the list had no criminal record or warrant and were not suspected of a crime already committed.[5] How did the Chicago

---

[1] *See* CIVIL RIGHTS, BIG DATA, AND OUR ALGORITHMIC FUTURE [heretofore "BIG DATA FAIRNESS REPORT"] 18 (September 2014), https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-Algorithmic-Future-v1.2.pdf.

[2] These visits are called "custom notifications." GARRY F. MCCARTHY, CUSTOM NOTIFICATIONS IN CHICAGO – PILOT PROGRAM D13-09, http://directives.chicagopolice.org/directives-mobile/data/a7a57bf0-13fa59ed-26113-fa63-2e1d9a10bb60b9ae.html?ownapi=1 (last visited Nov. 4, 2015).

[3] *Id.; see also* Tony Dokoupil, *'Small World of Murder': A Homicides Drop, Chicago Police Focus on Social Networks of Gangs*, NBC NEWS, http://www.nbcnews.com/news/other/small-world-murder-homicides-drop-chicago-police-focus-social-networks-f2D11758025.

[4] *See* BIG DATA FAIRNESS REPORT, *supra* note 1; McCarthy, *supra* note 2; Dokoupil, *supra* note 3; Jay Stanley, *Chicago Police "Heat List" Renews Old Fears About Government Flagging and Tagging*, AM. CIVIL LIBERTIES UNION: FREE FUTURE BLOG (Feb, 25, 2014), https://www.aclu.org/blog/chicago-police-heat-list-renews-old-fears-about-government-flagging-and-tagging.

[5] *See, e.g.*, John Eligon & 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 (reporting on similar programs in Kansas City and other areas); Anna Maria Barry-Jester et al., *The New Science of Sentencing*, THE MARSHALL PROJECT (Aug. 4, 2015), https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing (explaining a new sentencing program considered in Pennsylvania that would use predictive analytics to determine whom to parole based on likelihood of committing future crimes); 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-

Police Department determine who was most likely to commit a crime? The list was compiled by a predictive policing model —a computer algorithm that uses big data and machine learning to predict future criminal activity.[6] These models, developed and sold by private companies, have become increasingly popular among local law enforcement agencies.[7] Police departments promote the ability of predictive policing models to reduce crime,[8] but few details about how the models work and what data they use have been released to the public.[9]

In Fresno, California, a predictive program called Beware assigns "threat scores" to individuals who call 911.[10] The score—red, yellow, or green—is displayed to the 911 operator so that responders can prepare for potentially dangerous encounters.[11] Beware

---

algorithm-minority-report (describing the Los Angeles Police Department's use of PredPol's predictive policing software, which uses weather prediction technology to map and forecast crime by neighborhood).

[6] *See* Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L. J. 259, 265 (2012). Ferguson's research focuses on predictive policing tools that map crime and attempt to forecast the neighborhoods where particular types of crime are most likely to occur. *See generally Id.* These crime mapping functions are different from the models this thesis discusses, which target individuals rather than geographic areas, but both types of tools fall under the predictive policing umbrella.

[7] *See, e.g.*, John Eligon & Timothy Williams, *Police Program Aims to Pinpoint Those Most Likely to Commit Crimes*, N.Y. TIMES (Sept. 24, 2015), http://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html (reporting on similar programs in Kansas City and other areas); Anna Maria Barry-Jester et al., *The New Science of Sentencing*, THE MARSHALL PROJECT (Aug. 4, 2015), https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing (explaining a new sentencing program considered in Pennsylvania that would use predictive analytics to determine whom to parole based on likelihood of committing future crimes); 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 (describing the Los Angeles Police Department's use of PredPol's predictive policing software, which uses weather prediction technology to map and forecast crime by neighborhood).

[8] Dokoupil, *supra* note 3 (describing Chicago police leaders expressing optimism about their social network gang audits, jokingly referring to their "pre-crime unit," and "radiating . . . a glow more often found onstage at TED talks").

[9] *See, e.g.*, BIG DATA FAIRNESS REPORT, *supra* note 1.

[10] *Id.*; David Robinson, *Buyer Beware: A Hard Look at Police 'Threat Scores'*, EQUALFUTURE (Jan. 14, 2016), https://www.equalfuture.us/2016/01/14/buyer-beware-police-threat-scores/.

[11] *See* Robinson, *supra* note 10.

uses information from commercial data brokers, which comb the Internet and compile available data on individuals.[12] This can include everything from criminal records to social media activity to health information.[13]

Predictive policing models are the latest step in a long history of attempts by law enforcement to predict and prevent crime before it occurs.[14] There are different types of predictive policing tools, but this thesis focuses on those that analyze large data sets to determine the probability that an individual will commit a crime. Because these predictions occur before any criminal activity is observed or reported, they rely on facts that are facially innocent—such as personal relationships[15] or employment status[16]—that are nonetheless statistically associated with crime.[17] Suspicion based on facially innocent activity is not a new concept. For decades, police have used crime "profiles" to justify investigative stops.[18] For example, law enforcement agencies have developed a "drug

---

[12] *Id.*

[13] *Id.*

[14] For example, in *Terry v. Ohio*, the Supreme Court recognized the need for "effective crime prevention and detection" when it created a category of law enforcement investigative stops, which fall short of full arrests, that fall outside of the usual Fourth Amendment warrant or probable cause requirement. Terry v. Ohio, 392 U.S. 1, 22 (1968). In the 1990s, the New York Police Department ("NYPD") introduced the Compstat system, which encompassed multiple data-driven methods of attempting to reduced crime. *See generally* VINCENT E. HENRY, THE COMPSTAT PARADIGM: MANAGEMENT ACCOUNTABILITY IN POLICING, BUSINESS AND THE PUBLIC SECTOR (2003); ELI B. SILVERMAN, NYPD BATTLES CRIME: INNOVATIVE STRATEGIES IN POLICING 97-124 (1999).

[15] The Chicago Police Department ("CPD") reportedly uses "social network analysis" to map individuals' associations, especially within gangs, to create its predictions. Dokoupil, *supra* note 3.

[16] *See* Anna Maria Barry-Jester et al., *supra* note 7 (providing a sample risk assessment form for parole candidates that includes employment status, among other factors).

[17] *See* Ferguson, *supra* note 6, at 309.

[18] United States v. Sokolow, 490 U.S. 1, 9–10 (1989) ("Any one of these factors [provided by the police as justification for a stop] is not by itself proof of any illegal conduct and is quite consistent with innocent travel. But we think taken together they amount to reasonable suspicion. . . . Indeed, *Terry* [*v. Ohio*] itself involved 'a series of acts, each of them perhaps innocent' if viewed separately, 'but which taken together warranted further investigation.' . . . '[i]n making a determination of [reasonable suspicion] the relevant

courier profile"—a list of characteristics and behaviors associated with people transporting narcotics—and routinely stop people in airports who appear to fit these profiles.[19] The drug courier profile consists of behaviors such as being the first to deplane a flight, not checking baggage, and appearing sweaty—facially innocent behaviors that, taken together, may indicate a narcotics trafficker. This logic of associating innocent activity with criminal acitivity also underlies the predictive policing models discussed in this thesis. Thus, those predictive policing models can be described as "automated profiling" models.

Police have used automated profiling as a basis for initiating contact with individuals.[20] In general, police contact ranges from consensual encounters, for which no suspicion is required under the Fourth Amendment;[21] to investigative or "Terry" stops, which require reasonable and articulable suspicion;[22] to arrests, which require probable cause.[23] Traditional analog profiling generally results in investigative stops.[24] In a typical profiling case, an officer on patrol observes behavior or characteristics that match a profile and stops the observed individual for questioning. Thus, the constitutionality of profiling has been analyzed primarily under the reasonable and articulable suspicion

---

inquiry is not whether particular conduct is "innocent" or "guilty," but the degree of suspicion that attaches to particular types of noncriminal acts.'").

[19] *See, e.g.*, *Sokolow*, 490 U.S. 1; United States v. Mendenhall, 446 U.S. 544 (1980); Reid v. Georgia, 448 U.S. 438 (1980); Florida v. Royer, 460 U.S. 491 (1983); Ornelas v. United States, 517 U.S. 690 (1996).

[20] *See* Dokoupil, *supra* note 3; Erica Goode, *Sending the Police Before There's a Crime*, New York Times (Aug. 15, 2011), http://www.nytimes.com/2011/08/16/us/16police.html.

[21] *See* WAYNE R. LAFAVE ET AL., 2 CRIMINAL PROCEDURE § 3.8(c) (3d ed. 2014) (describing action short of a stop).

[22] *Terry*, 392 U.S. at 27.

[23] *See generally id.*

[24] *See, e.g.*, United States v. Sokolow, 490 U.S. 1 (1989).

standard.[25] This standard asks whether the totality of the circumstances led to an officer's reasonable inference that "criminal activity [was] afoot."[26] Under this standard, the Supreme Court has given law enforcement broad leeway to use police-developed crime profiles as a basis for making investigative stops.[27]

However, automated profiling differs from analog profiling in significant ways. Automated profiling involves both human value judgments and computer learning in a continually evolving process of developing and fine-tuning profiles.[28] First, programmers must write the underlying algorithm that will analyze datasets and make predictions.[29] These models are typically developed by private companies and licensed to police departments,[30] so there may be significant variations in these algorithms from one company to the next. Furthermore, the officers who use them may have little or no involvement in the development of the code and little control over or even knowledge of the underlying logic of the algorithms. Second, the models use computer learning to search for statistical associations and patterns in the data, which the models then use as rules to make future predictions.[31] This means that automated profiles can develop and change over time without any human intervention. Third, in order to predict crimes

---

[25] *See id.*
[26] *Id.* at 7–8.

[27] *See generally* Gregory Howard Williams, *The Supreme Court and Broken Promises: The Gradual But Continual Erosion of* Terry v. Ohio, 34 HOW. L. J. 467 (1991).

[28] *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. __, 6–7 (forthcoming 2016) (describing the process and objectives of data mining and the role that human value judgments play).

[29] *Id.*

[30] *See, e.g.*, PREDPOL, http://www.predpol.com/ (last visited Dec. 3, 2015); HUNCHLAB, https://www.hunchlab.com/ (last visited Dec. 3, 2015).

[31] See Barocas & Selbst, *supra* note 28, at 7–8 (describing "computer learning").

earlier—before any activity[32] is observed by a police officer—predictive algorithms are designed to find non-obvious connections between innocent facts and criminal activity. [33] Algorithms are designed to find correlations that human police officers would not have found through their own common sense and experience. Finally, as in Chicago, automated predictions will likely lead to police intervention before any behavior—innocent or criminal—is actually observed. Thus, automated profiling will increase the frequency of consensual police encounters, which fall outside of Fourth Amendment suspicion requirements.

These changes all have the potential to impact law enforcement accountability, transparency, and fairness. They also raise questions about whether the Fourth Amendment applies differently to criminal investigative techniques involving automated profiling and, if so, how. The purpose of this thesis is to explore the legal and policy challenges raised by predictive policing practices that involve automated profiling. Chapter I reviews the existing literature on law enforcement investigative profiling, automated decision-making systems, and predictive policing. Chapter I also presents the research questions this thesis will answer, the methodology it will use to answer those questions, and the limitations of this research. Chapter II analyzes how federal appellate courts have applied Fourth Amendment law to analog profiling. Chapter III discusses how these Fourth Amendment principles might apply to automated profiling and the new interpretational challenges that automated profiling will present for courts reviewing Fourth Amendment challenges to profile-based stops. Chapter IV moves away from legal

[32] Criminal or innocent.

[33] *See generally, e.g.*, Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 Harv. L. & Pol'y Rev. 15 (2016).

analysis to discuss some of the limitations and public policy issues that should be considered before automated profiling models are adopted. Finally, Chapter V summarizes the findings of this research, suggests some policy guidelines for minimizing the potential harms associated with automated profiling, and proposes questions for further research.

Literature Review

This thesis intersects two areas of scholarly interest: law enforcement criminal profiling and automated decision-making systems. Sections I and II review the relevant literature on these topics. Section III reviews the existing legal scholarship discussing predictive policing, which consists of only one in-depth analysis. This thesis builds on the small body of work around predictive policing and fills a gap in both the profiling and the automated decision-making literature by analyzing predictive policing as a form of automated profiling.

<u>Law Enforcement Criminal Profiling—The Drug Courier Profile</u>

In the most basic sense, criminal profiling refers to the practice of investigating individuals for potential criminal activity based on generalized factors. This literature review focuses on formalized profiling practices—established law enforcement policies and practices that involve the explicit application of a pre-determined profile to individuals. Although predictive policing has the potential to involve more implicit or informal forms of profiling, such as racial profiling,[34] the vast literature on racial

[34] Later chapters of this thesis will discuss the potential for predictive policing to facilitate both intentional and unintentional racial profiling.

profiling is outside the scope of this literature review.[35] In the analog world, the drug courier profile is the best known formalized profiling practice. The drug courier profile has received ample attention from scholars and courts.[36] This is likely for two reasons: (1) drug courier profiling has been a commonplace law enforcement practice since at least the 1970s and has loomed large as part of a decades-long crackdown on illegal drug trafficking,[37] and (2) the drug courier profile, unlike other law enforcement practices, is relatively transparent.[38] The availability of information and jurisprudence around the drug courier profile makes it a helpful place to begin analyzing the Fourth Amendment implications of automated profiling. Thus, this literature review focuses on the scholarship discussing drug courier profiling.

The "drug courier profile" was developed in the 1970s by the Drug Enforcement Agency ("DEA") to help identify commercial air passengers suspected of carrying illegal

---

[35] For in-depth analyses and discussions of racial profiling, see, e.g., Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L. REV. 1 (1994); David A. Slansky, *Traffic Stops, Minority Motorists, and the Future of the Fourth Amendment*, 1997 SUP. CT. REV. 271 (1997); Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956 (1999); Samuel R. Gross & Debra Livingston, *Racial Profiling Under Attack*, 102 COLUM. L. REV. 1413 (2002); William J. Stuntz, *Race, Class, and Drugs*, 98 COLUM. L. REV. 1795 (1998); David A. Harris, *Factors for Reasonable Suspicion: When Black and Poor Means Stopped and Frisked*, 69 IND. L.J. 659 (1994); Angela J. Davis, *Race, Cops, and Traffic Stops*, 51 U. MIAMI L. REV. 425 (1997); Sheri Lynn Johnson, *Race and the Decision to Detain a Suspect*, 93 YALE L.J. 214 (1983).

[36] *See* Wayne R. LaFave, *Controlling Discretion by Administrative Regulations: The Use, Misuse, and Nonuse of Police Rules and Policies in Fourth Amendment Adjudication*, 89 MICH. L. REV. 442, 480 (1990) ("[I]n terms of frequency of use by law enforcement officers and frequency of confrontation by appellate courts, [no profile] matches the drug courier profile.").

[37] *See, e.g.*, Morgan Cloud, *Search and Seizure by the Numbers: The Drug Courier Profile and Judicial Review of Investigative Formulas*, 65 B. U. L. Rev. 843, 847–48 (1985); United States v. Mendenhall, 446 U.S. 544, 561–62 (1980) (Powell, J., concurring) ("Few problems affecting the health and welfare of our population, particularly our young, cause greater concern than the escalating use of controlled substances. . . . the obstacles to detection of illegal conduct may be unmatched in any other area of law enforcement.").

[38] Cloud, *supra* note 37, at 878–79.

narcotics.[39] Typically, DEA agents and police officers observe arriving and departing airline passengers, watching for characteristics and behavioral traits that, "on the basis of [police officers'] collective experience, have tended to distinguish drug couriers from other passengers."[40]

> When a specific traveler arouses the agents' suspicions, [the agents] approach the suspect, identify themselves, ask the suspect to consent to questioning, and ask to see the suspect's identification and ticket. If the agents' suspicions are not eliminated during this exchange, they continue to question the suspect and ask him to move to another location within the airport, often a room used by law enforcement officers. The suspect is typically asked at this point to consent to a search of his person, luggage, or both. If the suspect voluntarily consents to the police requests at any stage of the transaction, the police are free to continue the investigation. If the suspect does not consent and attempts to depart, the police must either allow him to proceed on his way or seize him.[41]

This literature review will address three common criticisms of the drug courier profile: (1) that its lack of uniformity makes it unreliable and gives police too much discretion;[42] (2) that it provides only generalized suspicion, rather than the individualized suspicion that the Fourth Amendment requires;[43] and (3) that the judiciary abdicates its duty to

---

[39] *See* Cloud, *supra* note 37, at 844; United States' Petition for Cert. at 2–3 & n.1, *Mendenhall*, 446 U.S. 544; United States v. Ehlebracht, 693 F.2d 333, 335 n.3 (5th Cir. 1982) (identifying DEA Special Agent Paul Markonni as the creator of the drug courier profile).

[40] United States' Petition for Cert. at 3, *Mendenhall*, 446 U.S. 544; *see also* Cloud, *supra* note 37, at 848.

[41] Cloud, *supra* note 37, at 848–49 (citing United States' Petition for Cert. at 3, *Mendenhall*, 446 U.S. 544; Florida v. Royer, 460 U.S. 491, 493–95 (1983); Reid v. Georgia, 448 U.S. 438, 439 (1980); *Mendenhall*, 446 U.S. at 547; United States Petition for Cert. at 12, *Mendenhall*, 446 U.S. 544; United States v. Bailey, 691 F.2d 1009, 1011–12 (11th Cir.1982), *cert. denied*, 461 U.S. 933 (1983); United States v. Van Lewis, 409 F. Supp. 535, 538–39 (E.D. Mich. 1976), *aff'd* 556 F.2d 385 (6th Cir. 1977), *cert. denied*, 434 U.S. 1011 (1978); Brief for the United States 2–4, *Mendenhall*, 446 U.S. 544; Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973); Terry v. Ohio, 392 U.S. 1 (1968)).

[42] *See infra* notes 50–57 and accompanying text.

[43] *See infra* notes 58–68 and accompanying text.

conduct individualized Fourth Amendment review when it accepts the profile as evidence of reasonable and articulable suspicion.[44]

Validity and Accountability

The Supreme Court has neither explicitly accepted nor prohibited law enforcement's use of the drug courier profile to justify brief investigative seizures.[45] Morgan Cloud's 1985 article, *Search and Seizure by the Numbers: The Drug Courier Profile and Judicial Review of Investigative Formulas*, criticized the Court for deciding drug courier profile cases without delineating the specific characteristics that make up the profile or assessing its empirical validity.[46] For an operational definition of the drug courier profile, Cloud pointed to the original profile created by DEA Special Agent Paul Markonni:

> The primary characteristics are: (1) arrival from or departure to an identified source city; (2) carrying little or no luggage, or large quantities of empty suitcases; (3) traveling by an unusual itinerary, such as a rapid turnaround time for a very lengthy airplane trip; (4) use of an alias; (5) carrying unusually large amounts of currency in the many thousands of dollars, usually on the suspect's person, in briefcases or bags; (6) purchasing airline tickets with a large amount of small denomination currency; and

---

[44] *See infra* notes 69–73 and accompanying text.

[45] *See* United States v. Sokolow, 490 U.S. 1, 10 (1989); *see also* Cloud, *supra* note 37, at 851 (citing *Royer*, 460 U.S. at 512 (Brennan, J., concurring); *Reid*, 448 U.S. at 441; and *Mendenhall*, 446 U.S. at 572 (White, J., dissenting), for the proposition that "[s]ome Justices [] have argued that the drug courier profile characteristics cannot provide reasonable suspicion"); *id.* (citing United States v. Harrison, 667 F.2d 1158, 1161 (4th Cir. 1982); United States v. $73,277, United States Currency, 710 F.2d 283, 290–91 (7th Cir. 1983); and United States v. Ehlebracht, 693 F.2d 333, 337 (5th Cir. 1982), for the proposition that "Other[] [judges] have concluded that while drug courier profile characteristics alone do not supply reasonable suspicion, they may when supplemented by additional suspicious facts"); *id.* (citing *Royer*, 460 U.S. at 525 (Rehnquist, J., dissenting); United States v. Viegas, 639 F.2d 42 (1st Cir.); and United States v. Forero-Rincon, 626 F.2d 218 (2d Cir. 1980), for the proposition that "[a] third group [of judges] contends that the drug courier profile characteristics alone are sufficient"). Note that Cloud wrote this article before *Sokolow* was decided.

[46] Cloud, *supra* note 37, at 843–47; *see also* LaFave, *supra* note 36, at 481–82.

> (7) unusual nervousness beyond that ordinarily exhibited by passengers.
>
> The secondary characteristics are: (1) the almost exclusive use of public transportation, particularly taxicabs, in departing from the airport; (2) immediately making a telephone call after deplaning; (3) leaving a false or fictitious callback telephone number with the airline; and (4) excessively frequent travel to source or distribution cities.[47]

The other predominant profile, according to Cloud, was articulated in *United States v. Ballard*[48]:

> The eleven characteristics [of the *Ballard* profile] are (1) unusual nervousness; (2) no luggage or very limited luggage; (3) possession of an unusually large amount of cash, especially when in bills of small denominations; (4) unusual itinerary, such as taking circuitous routes from cities known to be source cities for narcotics; (5) arriving from a known narcotics source city; (6) paying for an airline ticket in currency of small denominations; (7) purchasing a one-way ticket; (8) use of an alias; (9) use of a false telephone number on an airline reservation; (10) placing a telephone call immediately upon arrival at the airport; and (11) travel by a known narcotics trafficker.[49]

However, Cloud pointed out that the drug courier profile characteristics articulated by police officers often vary from case to case, making the profile "chameleon-like."[50]

The malleable nature of the drug courier profile has drawn criticism from several scholars and judges.[51] They have argued that the profile's malleability makes its accuracy

---

[47] Cloud, *supra* note 37, at 871 (citing United States v. Elmore, 595 F.2d 1036, 1039 n.3 (5th Cir. 1979), *cert denied*, 447 U.S. 910 (1980)). LaFave also points to the *Elmore* profile as the most commonly confronted profile. LaFave, *supra* note 36, at 480.

[48] 573 F.2d 913 (5th Cir. 1978).

[49] Cloud, *supra* note 37, at 872 (citing *Ballard*, 573 F.2d at 914).

[50] *Id.* 879.

impossible to verify[52] and gives individual police officers too much discretion.[53] Christopher Slobogin has criticized the "post-hoc nature of the so-called 'profiles'"—the fact that officers make them up after-the-fact to justify a seizure.[54] However, Slobogin wrote that "if a profile is proven to show the requisite correlation with crime, and it is clear that the profile was actually used by the police in deciding to act, rather than made up afterward, then its use should not be prohibited."[55] Wayne R. LaFave has similarly cautioned that "[b]efore courts readily accept [drug courier profile] guideline[s], they are [] 'obliged to require that the government provide satisfactory empirical evidence that the profile is valid and actually works.'"[56] LaFave also noted that "the profiles do not predetermine just what combination of suspicious factors must exist for a lawful stop, an especially critical matter given that some of those factors . . . 'describe a very large category of presumably innocent travelers.'"[57]

Generalized Versus Individualized Suspicion

The drug courier profile led the Supreme Court to decide for the first time, in *United States v. Sokolow*,[58] that police could stop an individual based on behavior or

---

[51] *See Id.;* LaFave, *supra* note 36, at 482; David Cole, *Discretion and Discrimination Reconsidered: A Response to the New Criminal Justice Scholarship*, 87 GEO. L. J. 1059, 1077 (1999); United States v. Sokolow, 831 F.2d 1413, 1418 (9th Cir. 1987), *rev'd*, United States v. Sokolow, 490 U.S. 1 (1989); Grant v. State, 461 A.2d 524, 526 (Md. App. 1983).

[52] *See, e.g.*, LaFave, *supra* note 36, at 480–82.

[53] *See, e.g., Id.* at 482–83; Cole, *supra* note 51.

[54] Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 81 (1991).

[55] *Id.* at 82.

[56] LaFave, *supra* note 36, at 481–82 (quoting Cloud, *supra* note 37, at 873).

[57] *Id.* at 482–83 (quoting Reid v. Georgia, 448 U.S. 438, 441 (1980)).

[58] 490 U.S. 1 (1989).

characteristics consistent with innocent conduct.[59] Slobogin seemed to agree[60] with the *Sokolow* majority's dual justifications: (1) that this standard followed precedent, since the Court had previously upheld *Terry* stops based on conduct susceptible to an innocent explanation;[61] and (2) that officers' training and experience allow them to interpret conduct as indicative of crime although it may seem innocent to an untrained bystander.[62] Cloud, however, argued that the drug courier profile was different from other bases for suspicion; its general nature could not support individualized suspicion.[63] Cloud argued that the drug courier profile raises "difficult Fourth Amendment issues" because it "describes innocent behaviors not linked to any specific crime. . . . compounded by the fact that these innocuous behaviors undoubtedly are exhibited by a large number of innocent travelers."[64] Cloud acknowledged that "the police sometimes are justified in relying upon ostensibly innocent conduct to justify searches and seizures," but he argued that drug courier profile methodology "differs from previously accepted police practices": "The profile does not identify conduct [that] is peculiar to a particular crime or suspect. Instead[,] it focuses on general patterns of behavior."[65]

---

[59] United States v. Sokolow, 490 U.S. 1, 9 (1989) ("Any one of these factors is not by itself proof of any illegal conduct and is quite consistent with innocent travel. But we think taken together they amount to reasonable suspicion.").

[60] *See* Slobogin, *supra* note 54, at 84 (pointing out that the facts in Camera v. Municipal Court, 387 U.S. 523 (1967) were "as 'innocent' as those found in a drug courier profile").

[61] *Sokolow*, 490 U.S. at 10.

[62] *Id.* at 10.

[63] Cloud, *supra* note 37, at 853.

[64] *Id.* at 852; *see also* Cole, *supra* note 51, at 1077 ("[T]he drug courier profile is said to be a compilation of police experience about who is more likely to be carrying drugs.").

[65] Cloud, *supra* note 37, at 852. For example, peering into car windows is said to be susceptible to an innocent explanation but is also indicative of automobile theft. But this behavior is directly related to the crime because it indicates an attempt to scope out automobiles for theft. Cloud seemed to argue that drug

Slobogin responded to Cloud's criticism of the "generalized" nature of the drug courier profile.[66] Slobogin argued that "a person targeted by a profile *is* being stopped for characteristics or actions specific to that individual, such as nervous appearance, choice of luggage, and choice of flights (factors which, taken together, happen to correlate at a particular level with being a drug courier)."[67] He contended that Cloud's argument, if carried to its logical conclusion, "would circumscribe many accepted types of police action. For instance, the suspicion underlying the detention of a person believed to be a potential criminal is often based on police experience with previous crimes under similar circumstances."[68]

Effect on Fourth Amendment Judicial Review

Cloud worried that the drug courier profile would fundamentally alter Fourth Amendment judicial review because judges would mechanically base their reasonable suspicion analyses upon whether the defendant's behavior was matched to a drug courier profile. Cloud also contended that acceptance of the drug courier profile violated a "basic premise of [Fourth Amendment] judicial review," that "each case raising a Fourth Amendment issue must be judged on its own facts."[69] In Cloud's view, the profile represents an unconstitutional "litmus-paper test," developed by police officers

courier profiles are made up of factors that aren't directly related to the act of transporting illegal narcotics but that were merely observed in known drug traffickers.

[66] Slobogin, *supra* note 54, at 82–83.

[67] *Id.* at 83.

[68] *Id.*

[69] Cloud, *supra* note 37, at 856 (quoting United States v. Mendenhall, 446 U.S. 544, 565 n.6 (1980)) (alterations omitted).

themselves, to determine whether police possessed sufficient facts to justify a seizure.[70] Cloud wrote that "[a]cceptance of a formula allegedly answering [F]ourth [A]mendment questions would radically alter the judiciary's role. Judges would no longer engage in an independent review of the facts, but would be relegated to monitoring the use of investigative formulas by the police . . . ."[71] Cloud pointed to several factors that would make this lack of judicial review problematic: the lack of scientific evidence validating the drug courier profile; the fact that the profile is used to evaluate complex human behaviors rather than simple scientific facts; and the fact that the profile is used to answer questions of constitutionality in felony cases where ultimate liberty issues are at stake.[72] Cloud concluded that "[t]he most rational judicial response to the profile would be to ignore it and rely instead upon the traditional methodology of the [F]ourth [A]mendment in deciding individual cases."[73]

Conclusion

Many of the concerns scholars voiced about the drug courier profile apply to predictive policing to an even greater degree. Like drug courier profiles, the profiles used in predictive policing represent generalized observations about a class of known criminals.[74] Unlike drug courier profiles, however, police officers would not be able to

[70] *Id.* at 857.

[71] *Id.*

[72] *Id.* at 858.

[73] *Id.* at 920.

[74] These algorithms could be even more generalized than drug courier profiles because they cannot take into account a suspect's real-world behavior during ongoing criminal activity, such as appearing nervous. Instead, they have to rely on information that police have about a person before any activity is observed. This concern may be compounded by the fact that algorithms are designed to look for non-obvious patterns. If the relationship between a facially innocent characteristic and a particular crime is not ascertainable by a police officer without using data mining tools, the connection is likely remote. In predictive policing, this

alter the predictive algorithm to fit a particular observation. This arguably makes predictive algorithms easier to empirically validate than more amorphous analog profiles. However, Cloud's concerns about judicial review are eerily applicable. Scholars are already calling on courts to adopt reliability standards for predictive policing tools. If courts allow automated predictions to justify Fourth Amendment seizures, individualized Fourth Amendment inquiries could give way to mechanistic applications of predetermined technological[75] standards.[76]

<u>Automated Decision Making</u>

Predictive policing is just one of many applications of automated decision making.[77] The government and private companies use predictive algorithms to determine who is creditworthy,[78] who qualifies for social programs,[79] what ads to display to Internet users,[80] and whom to hire.[81] This section will review the scholarship discussing legal and policy issues raised by automated decision making. Part A gives an overview of the basic concepts and terms underlying automated decision-making systems as well as some of the applications of automated decision making. Part B covers the common misconception

---

design is purposeful. A question for our courts and for the public is whether we want to allow police to stop and question individuals based on facially innocent factors that even a trained and experienced officer would not have associated with crime.

[75] As opposed to legal.

[76] Standards that, even if reviewed and approved by judges, will likely be set forth by law enforcement agencies or commercial industries.

[77] *See, e.g.*, *infra* notes 91–93 and accompanying text.

[78] *See infra* note 88 and accompanying text.

[79] *See, e.g.*, *infra* notes 91–92 and accompanying text.

[80] *See, e.g.*, Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMMS. OF THE ACM 44, 47–48 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240&download=yes (discussion of Google Adsense).

[81] *See, e.g.*, infra notes 93, 96, 108–09 and accompanying text.

that data mining is neutral and discusses the ways in which this process can discriminate against certain classes. Finally, Part C addresses the lack of transparency of automated decision-making systems and the implications of this opacity on accountability and due process.

Data Mining for Automated Decision Making: Definitions and Practices

Automated decision-making systems are algorithms that analyze or "mine" large data sets, usually for the purpose of categorizing individuals (for example, as creditworthy or not creditworthy).[82] Solon Barocas and Andrew D. Selbst have aptly described how these systems work:

> In contrast to those traditional forms of data analysis that simply return records or summary statistics in response to a specific query, **data mining** attempts to locate statistical relationships in a dataset. In particular, it automates the process of discovering useful patterns, revealing regularities upon which subsequent decision-making can rely. The accumulated set of discovered relationships is commonly called a "**model**," and these models can be employed to automate the process of classifying entities and activities of interest, estimating the value of unobserved variables, or predicting future outcomes. . . . [This process] involve[s] attempts to determine the status or likely outcome of cases under consideration based solely on access to *correlated* data.[83] Data mining helps identify cases of spam and fraud and anticipate default and poor health by treating these states and outcomes as a function of some other set of observed characteristics. In particular, by exposing so-called **"machine learning" algorithms** to examples of the cases of interest[,] . . . the algorithm "learns" which related attributes or activities can serve as potential proxies for those qualities or outcomes of interest. In the machine

[82] *See generally* Barocas & Selbst, *supra* note 28, at 7–8.

[83] Note again the similarities between automated decision making and analog criminal profiling. Both rely on correlations between observed characteristics (e.g., looking nervous) and unobserved or unobservable qualities (e.g., intent to commit a crime).

> learning and data mining literature, these states or outcomes of interest are known as "**target variables**."[84]

The cases that algorithms use to "learn," or to look for relationships in the data, are called "**training data**."[85] Barocas and Selbst pointed out that

> [b]y definition, data mining is *always* a form of statistical (and therefore seemingly rational) discrimination. Indeed, the very point of data mining is to provide a rational basis upon which to distinguish between individuals and to reliably confer to the individual the qualities possessed by those who seem statistically similar.[86]

Scholars have noted the increasing reliance on automated decision-making systems in the public and private sectors.[87] Barocas and Selbst list three common applications: "fraud detection, credit scoring, and insurance pricing,"[88] and their analysis focuses on automated decisions about whom to hire.[89] Danielle Keats Citron's article, *Technological Due Process*, analyzes the use of automated decision-making by federal agencies, which use these models to apply agency rules to individual cases.[90] The models perform tasks such as "identify[ing] students eligible for free or reduced-price school

---

[84] *Id.* at 7–8; *see* COMMITTEE ON THE ANALYSIS OF MASSIVE DATA, ET AL., FRONTIERS IN MASSIVE DATA ANALYSIS 66–69 (2013), http://bigdatawg.nist.gov/FrontiersInMassiveDataAnalysisPrepub.pdf (emphasis added, bolded terms only).

[85] Barocas & Selbst, *supra* note 28, at 10.

[86] *Id.* at 7.

[87] *See infra* notes 88–93 and accompanying text.

[88] Barocas & Selbst, *supra* note 28, at 7.

[89] *See id.* at 9.

[90] Danielle Keats Citron, *Technological Due Process*, 85 WASH. L. REV. 1249, 1263 (2008).

lunches"[91] and "enroll[ing] eligible senior citizens into Medicare coverage."[92] In Keats's and Frank Pasquale's article, *The Scored Society*, they list the following examples of judgments made by predictive algorithms:

> Job candidates are ranked by what their online activities say about their creativity and leadership. Software engineers are assessed for their contributions to open source projects, with points awarded when others use their code. Individuals are assessed as likely to vote for a candidate based on their cable-usage patterns. Recently released prisoners are scored on their likelihood of recidivism.[93]

The literature catalogs widespread use of predictive algorithms to make crucial decisions that significantly impact people's lives. This phenomenon is ripe for analysis.

The Myth of Neutrality and the Potential for Big Data Discrimination

Barocas and Selbst devote much of their article to busting the myth that data mining is neutral.[94] They catalog the ways in which bias can enter the data mining process and lead to discrimination. First, human subjectivity plays a role in designing the

---

[91] *Id.* (citing U.S. DEP'T OF AGRICULTURE, DATA MATCHING IN THE NATIONAL SCHOOL LUNCH PROGRAM 13 (2007), http://www.fns.usda.gov/oane/MENU/Published/CNP/FILES).

[92] *Id.* (citing STAN DORN & GENEVIEVE M. KENNEY, AUTOMATICALLY ENROLLING ELIGIBLE CHILDREN AND FAMILIES INTO MEDICAID AND SCHIP: OPPORTUNITIES, OBSTACLES, AND OPTIONS FOR FEDERAL POLICYMAKERS 5 (2006).

[93] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 2–3 (2014) (citing Don Peck, *They're Watching You at Work*, ATLANTIC MONTHLY (Dec. 2013), http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/ (describing the "emerging practice of 'people analytics'"); E. GABRIELLA COLEMAN, CODING FREEDOM 116–22 (2013) (exporing Debian open source community and assessment of community members' contributions); Alice E. Marwick, *How Your Data are Being Deeply Mined*, N.Y. REV. BOOKS (Jan. 9, 2014), http://www.nybooks.com/articles/2014/01/09/how-your-data-are-being-deeply-mined/; Danielle Keats Citron, *Data Mining for Juvenile Offenders*, CONCURRING OPINIONS (Apr. 21, 2010, 3:56 PM), http://concurringopinions.com/archives/2010/04/data-mining-for-juvenile-offenders.html (discussing an announcement by the Florida State Department of Juvenile Justice that it would use IBM predictive analytics software to reduce recidivism)).

[94] *See, e.g.*, Barocas & Selbst, *supra* note 28, at 1 ("Big data claims to be neutral. It isn't.").

algorithm.[95] The target variable that the algorithm is supposed to determine (e.g., creditworthiness, good employee, likely recidivist criminal) must be operationalized as variables that algorithms can discern (e.g., good credit history, positive reviews on LinkedIn, low education level).[96] "Through this necessarily subjective process of translation, [] data miners may unintentionally parse the problem and define the target variable in such a way that protected classes happen to be subject to systematically less favorable determinations."[97] Citron described the same problem in a different way.[98] In the federal agency context, she wrote that "[c]omputer programmers inevitably engage in rulemaking" when they translate agency rules into code (which ultimately determines outcomes).[99] However, this type of rulemaking happens without the notice and review required of traditional rulemaking.[100]

Another way that bias can enter the automated decision-making process is through biased training data:

> [I]f data mining treats cases in which prejudice has played some role as valid examples from which to learn a decision-making rule, that rule may simply reproduce the prejudice involved in these earlier cases; and [] if data mining draws inferences from a biased data sample of the populations to which the inferences are expected to generalize, any decision that rests on these inferences may

---

[95] *Id.* at 7–8.

[96] *Id.*

[97] *Id.* at 8.

[98] *See* Citron, *supra* note 90, at 1288.

[99] *Id.*

[100] *Id.*

> systematically disadvantage those who are under- or over-represented in the dataset.[101]

Kate Crawford offered a real-world example of this problem in her article, *Think Again: Big Data*.[102] Crawford pointed to Street Bump, an application that detects and reports potholes in Boston by collecting data from residents' smart phones as they drive through the city.[103] Crawford warned that "whatever information the city receives from this application will be biased by the uneven distribution of smartphones across populations in different parts of the city."[104] This could result in underreporting, and potentially slower or fewer repairs, of road problems in poorer communities.[105]

Barocas and Selbst also warned of proxies for race and class that may be introduced into the algorithm.[106] This happens when "criteria that are genuinely relevant in making rational and well-informed decisions also happen to serve as reliable proxies for class membership."[107] These proxies tend to reveal existing and historical inequalities. In Barocas and Selbst's employment example, members of traditionally marginalized classes are more likely to lack the traditional markers associated with likely job success, such as education from an elite institution.[108] Thus:

---

[101] *See* Barocas & Selbst, *supra* note 28, at 10–11.

[102] Kate Crawford, *Think Again: Big Data*, FOREIGN POL'Y (May 10, 2013), http://foreignpolicy.com/2013/05/10/think-again-big-data/.

[103] *Id.*; *see* STREET BUMP, http://www.cityofboston.gov/DoIT/apps/streetbump.asp (last visited December 3, 2015).

[104] Barocas & Selbst, *supra* note 28, at 15 (citing Crawford, *supra* note 98).

[105] *Id.* (citing Crawford, *supra* note 98).

[106] *Id.* at 20–21.

[107] *Id.* at 21.

[108] *Id.*

> [E]mployers may find, in conferring greater attention and opportunities to employees that they predict will prove most competent at some task, that they subject members of protected groups to consistently disadvantageous treatment because the criteria that determine the attractiveness of employees happen to be held at systematically lower rates by members of these groups. Decision-makers do not necessarily intend this disparate impact because they hold prejudicial beliefs; rather, their reasonable priorities as profit-seekers unintentionally recapitulate the inequality that happens to exist in society.[109]

These potential entry points for discrimination may help explain the results of a 2013 empirical study by Latanya Sweeney.[110] Sweeney found that online searches for "black-sounding" names were more likely to yield ads suggesting that the person had an arrest record (e.g., reading "Latanya Farrell arrest record") than were searches for "white-sounding" names.[111] These ads are generated by Google's algorithm and are independent of any actual arrest records.[112] The study could not definitively answer why this was happening, but it showed that the algorithm was reflecting a societal racial bias, even if it did not accurately predict whether the person searched had been arrested.[113]

Transparency, Accountability, and Due Process

Throughout the automated decision-making literature, one concern seems to rise above the rest: a lack of transparency.[114] Citron and Pasquale warn that predictive

---

[109] *Id.*

[110] *See generally* Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMMS. OF THE ACM 44 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240&download=yes.

[111] *Id.* at 44.

[112] *Id.*

[113] *See generally Id.*

[114] *See, e.g.*, Citron, *supra* note 90, at 1254 ("The opacity of automated systems shields them from scrutiny. Citizens cannot see or debate these new rules. In turn, the transparency, accuracy, and political

algorithms are "zealously guarded" and "shrouded in secrecy," and therefore their decisions cannot be challenged.[115] In the government agency context, Citron argued that this raises due process issues, since rulemaking and adjudications are performed automatically without the requisite notice and opportunity for review.[116] Barocas and Selbst warned that algorithms may hide discrimination from even their own programmers.[117] Bias and discrimination in automated systems are often unintentional and thus difficult to detect.[118] When discrimination *is* intentional, Barocas and Selbst argued, it can be easily masked.[119] Indeed, scholars' reliance on hypothetical examples demonstrates a lack of public knowledge of the details of the predictive algorithms that determine our fates. Without adequate transparency, it is impossible to fully evaluate the effectiveness and shortcomings of automated decision-making systems.

Conclusion

Each of the concerns raised in the automated decision-making literature is relevant to the discussion of predictive policing models. While some authors mentioned policing generally, none of them has discussed the recent implementation of predictive

---

accountability of administrative rulemaking are lost."); Barocas & Selbst, *supra* note 28, at 1 ("[B]ecause the resulting discrimination is almost always an unintentional emergent property of the algorithm's use rather than a conscious choice by its programmers, it can be unusually hard to identify the source of the problem or to explain it to a court."); *Id.* at 23 ("[D]ata mining could provide cover for intentional discrimination . . . because the process would conceal from view that decision-makers had determined and considered the individual's class membership."); Citron and Pasquale, *supra* note 93, at 5 ("[S]coring systems are shrouded in secrecy. Although some scores, such as credit, are available to the public, the scorers refuse to reveal the method and logic of their predictive systems. No one can challenge the process of scoring and the results because the algorithms are zealously guarded trade secrets.").

[115] Citron and Pasquale, *supra* note 93, at 5.

[116] Citron, *supra* note 90, at 1254.

[117] Barocas & Selbst, *supra* note 28, at 1.

[118] *Id.*

[119] *Id.* at 22–24.

policing tools in police departments across the county. Very few legal scholars to date have specifically analyzed predictive policing practices. This scholarship will be discussed in the next section.

<u>Predictive Policing</u>

Two legal scholars, Andrew Guthrie Ferguson[120] and Elizabeth E. Joh,[121] have written about predictive policing. Joh's 2014 article, *Policing By Numbers: Big Data and the Fourth Amendment*, began to explore the interacting roles of artificial intelligence and human judgment in Fourth Amendment individualized suspicion.[122] Joh's analysis focused on predictions about the likely location of a future crime, and she concluded that "[w]hile likely not sufficient on its own to provide justification for a stop (because of its lack of specificity with regard to persons), such predictions could form the basis of police observation and corroboration."[123] She posited that courts are likely to accept automated predictions because the facts on which the predictions are based can be verified, making predictions arguably more objective than police officers' inferences and thus "likely to be a highly persuasive factor in the reasonable suspicion formulation."[124] However, Joh cautioned that "no predictive policing program is entirely objective."[125]

---

[120] Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012).

[121] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 Harv. L. & Pol'y Rev. 15 (2016); Elizabeth E. Joh, *Policing By Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014).

[122] Joh, *Policing By Numbers, supra* note 121, at 55.

[123] *Id.* at 57.

[124] *Id.*

[125] *Id.* at 58.

> The basic building blocks of a predictive software program necessarily involve human discretion. The assumptions underlying any method of crime prediction rely upon the decision to choose one model of risk prediction over another. The data used to build the models will depend on discretionary judgments about the types of crimes used for prediction, and the type of information used to predict those crimes.[126]

Joh also suggested that overreliance on probabilistic predictions might "nudge police judgments in favor of investigative detention in borderline cases because the police rely too heavily on probabilistic information."[127]

In her 2016 article, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, Joh argued that predictive policing tools gave police new capabilities to identify and focus surveillance on certain areas or suspects.[128] Joh labeled these decisions "surveillance discretion."[129] She argued that surveillance discretion has heretofore received little attention because "we assume that the police should possess such powers" and because surveillance discretion has been limited by the fact that investigations "typically only focus on a limited number of persons because of practical limitations imposed by resources and technology."[130] However, surveillance discretion capabilities will be expanded when "the ability to sort, score, and predict social activity will be an ordinary aspect of policing."[131] Joh suggested that we should rethink the lack

---

[126] *Id.*

[127] *Id.* at 58–59.

[128] Joh, *Surveillance Discretion*, *supra* note 121, at 15–19.

[129] *Id.* at 15.

[130] *Id.* at 17.

[131] *Id.* at 42.

of legal limitations on acts of surveillance discretion that fall short of Fourth Amendment searches and seizures.[132]

Ferguson has written two articles on predictive policing and Fourth Amendmetn reasonable suspicion. The first, *Predictive Policing and Reasonable Suspicion*, argued that automated predictions would likely be considered as part of the totality of the circumstances but would not be enough, standing alone, to satisfy reasonable suspicion.[133]

The legal scholarship addressing predictive policing is scarce. It largely focuses on geographic prediction models—those that predict where and what type of crime is likely to occur, but not who is likely to commit a crime.[134] The most cited work in this area is Andrew Guthrie Ferguson's *Predictive Policing and Reasonable Suspicion*.[135] As the title suggests, Ferguson explored how predictive policing might impact the Fourth Amendment reasonable and articulable suspicion analysis.[136] Ferguson's analysis also was limited to geographic predictions. He began with the premise that all non-warrant police seizures involve some type of prediction:

> Police officers regularly take action in anticipation of criminal activity. Stakeouts, ongoing surveillance, and undercover investigations focus not only on past crimes, but also future crimes. On the street, a *Terry* stop based on reasonable suspicion that "criminal activity may be afoot" is at base a prediction that the facts and circumstances

---

[132] *See generally id.*

[133] *See generally* Ferguson (2012), *supra* note 120.

[134] *See generally* Ferguson (2012), *supra* note 120.

[135] *Id.*

[136] *Id.*

> warrant the reasonable prediction that a crime is occurring or will occur.[137]

Ferguson then sought to determine whether a prediction generated by an algorithm might be individualized enough to support a finding of reasonable and articulable suspicion sufficient to justify a *Terry* stop.[138] In doing so, he analogized predictive policing to three existing lines of Fourth Amendment cases: tip cases, profile cases, and "high crime area" cases.[139]

Ferguson's analysis of Fourth Amendment cases revealed that (1) "the information [(tip, profile, or high crime area)] alone is never enough to control the reasonable suspicion analysis;" (2) "the predictive information must be particularized to a person, a profile, or a place, in a way that directly connects the suspected crime to the suspected person, profile, or place;" and (3) "the predictive value of the information declines over time, such that predictive information must be acted on quickly or be lost."[140] He concluded that "while insufficient on its own," a prediction that a particular type of crime was likely to occur in a particular area, "if corroborated" by a potential suspect's behavior (e.g., peering into car windows), "might result in reasonable suspicion."[141]

---

[137] *Id.* at 287.

[138] *Id.*

[139] *Id.* at 287–88.

[140] *Id.* at 303.

[141] *Id.* at 307.

In 2015, Ferguson followed up with a second article on predictive policing and reasonable suspicion.[142] In it, he argued that reasonable suspicion is a "small data" doctrine.[143] Reasonable suspicion is generally based on the few discrete facts that a police officer knows and/or observes about a potential suspect.[144] Ferguson noted that these pieces of information generally have not allowed police officers to learn the identity of the suspect before approaching him or her.[145] According to Ferguson, "[t]he wrinkle of big data is that now officers are no longer dealing with 'strangers.'"[146] Because automated prediction-based reasonable suspicion will be based on data about an individual rather than on his or her actions, Ferguson argued that reasonable suspicion will more often be based on innocent facts about individuals.[147] "Knowing who the suspect is and having more information (even innocent information) will allow the officer to meet the reasonable suspicion threshold more easily because the information will be sufficiently individualized and particularized."[148]

Ferguson's 2015 article argued for a big data solution to the Fourth Amendment challenges raised by big data and automated predictions.[149]

> If big data resources are used to tip the scales of reasonable suspicion in favor of law enforcement, then courts should require a higher level of detail and correlation using the

---

[142] Ferguson (2015), *supra* note 120.

[143] *Id.* at 329.

[144] *Id.*

[145] *Id.* at 329–30.

[146] *Id.* at 335.

[147] *Id.*

[148] *Id.*

[149] *Id.* at 336.

> insights and capabilities of big data. . . . Big data can provide information about a person on a generalized or granular scale, and the latter should be required. The power of big data allows investigators to go deep into the data and make sure that the information is as tightly correlated as possible. In this way, a big data-suspicion standard will do what the reasonable suspicion requirement was always supposed to do—distinguish the criminal from the noncriminal in a manner that balances the need for effective law enforcement with a measure of personal liberty.[150]

Conclusion

The existing legal scholarship on predictive policing has accepted that automated predictions will soon factor into the reasonable suspicion analysis. Scholars agree that courts must understand the capabilities and limitations of big data and automation so that Fourth Amendment rights are not violated. This thesis builds on existing scholarship by offering an in-depth exploration of how courts might apply Fourth Amendment reasonable suspicion principles to automated predictions. Unlike previous scholarship, this thesis focuses on predictions that determine an individual's likelihood of committing future crimes and analogizes this "automated profiling" to analog profiles such as the drug courier profile. This thesis also offers a much-needed discussion of the limits of these automated predictive models from a public policy perspective. Finally, this thesis offers a list of practical principles—in light of current and prospective uses of automated profiling—that law enforcement agencies, policymakers, and software developers should follow in order the minimize the potential harm of automated profiling to civil liberties.

Research Questions and Methodology

This thesis will address the following research questions:

[150] *Id.*

1. What have courts said about if or when using profiles as a basis for investigative stops violates the Fourth Amendment? What limits have they set on these practices?
2. What major problems does automated profiling present that the existing legal frameworks do not adequately address?
3. What limitations and policy considerations should data scientists, law enforcement agencies, and policymakers consider before designing, implementing, and regulating automated profiling models?
4. How can some of the problems identified in the answers to research questions two and three be addressed?

This thesis will review about 130 cases decided by the federal appellate courts that involve law enforcement's reliance on predetermined crime profiles to make investigative stops. Cases for analysis were identified by searching Westlaw. In order to limit the cases to those involving investigative stops (a concept defined in *Terry v. Ohio*), the pool of possible cases was limited to those citing *Terry*. Thus, the case dates range from 1968 to the present. Relevant cases were then found by filtering these citing references for cases containing the word "profile" or "profiling" and cases decided at the Supreme Court or circuit court levels. Cases in this group that obviously did not deal with profiling (e.g., referred to a "high-profile" case) were eliminated. Approximately 130 cases remained. Most of these cases involved some iteration of the "drug courier profile."

Limitations

This thesis has two major limitations. First, there is, as of now, no case law discussing predictive policing. Because the technology is new and has been implemented very recently, mostly in pilot programs, its use likely has not been challenged in court. For this reason, any legal analysis of predictive policing must attempt to draw analogies, in this case to profiling.

The most significant limitation for anyone writing about predictive policing is a lack of available information about the details of particular systems used by police. Neither private companies nor law enforcement agencies have released the details of how their algorithms work—what factors they associate with criminal activity, what databases they use, how they control for flawed data, etc. Thus, this analysis can only speculate about the functionality of these systems.

CHAPTER 2: PROFILING AND THE FOURTH AMENDMENT

Introduction

Law enforcement in the last half-century has been marked by ever-increasing emphasis on "ferreting out" crime before it occurs.[151] With this goal in mind, officers do not passively wait to observe criminal conduct but instead attempt to infer criminal activity from certain non-criminal observations.[152] As law professor Andrew Guthrie Ferguson has pointed out, such inferences are essentially predictions.[153] One such prediction is the "drug courier profile"—an "amalgam of characteristics" that is said to

[151] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 22 (1968) (establishing the law enforcement authority to perform brief investigative stops upon less than probable cause in the interest of "effective crime prevention and detection"); Sameer Bajaj, Note, *Policing the Fourth Amendment: the Constitutionality of Warrantless Investigatory Stops for Past Misdemeanors*, 109 COLUM. L. REV. 309, 317 (2009) ([*Terry*] [w]eighed against [the] privacy interest the governmental interest in 'effective crime prevention and detection'—i.e., the need to act quickly to foil imminent criminal activity . . . ."); *see generally* Lewis R. Katz, Terry v. Ohio *at Thirty-Five: A Revisionist View*, 74 MISS. L.J. 423 (2004) (explaining how *Terry*'s progeny has continued to expand the police power to stop individuals when police reasonably suspect that crime is afoot); *see also* Alexander H. Kipperman, Note and Comment, *Frisky Business: Mitigating Predictive Crime Software's Facilitation of Unlawful Stop and Frisks*, 24 TEMP. POL. & CIV. RTS. L. REV. 215, 217–220 (2014) (describing the development of CompStat in the 1990s, a sort of precursor to predictive policing software, as a way to use statistics and crime theories to attempt to predict and prevent crime).

[152] *See id.*; United States v. Sokolow, 490 U.S. 1, 9–10 (1989) ("We said in *Reid v. Georgia*, 'there could, of course, be circumstances in which wholly lawful conduct might justify the suspicion that criminal activity was afoot.' . . . We noted in *Gates* that 'innocent behavior will frequently provide the basis for a showing of probable cause[]' . . . . That principle applies equally well to the reasonable suspicion inquiry." (internal citations omitted)).

[153] Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 Emory L.J. 259, 262–63 (2012) ("Many aspects of current Fourth Amendment law are implicitly based on prediction. Search warrants are predictions that contraband will be found in a particular location. Investigative detentions are predictions that the person is committing, or about to commit, a crime. Fourth Amendment concepts like probable cause, reasonable suspicion, informant tips, drug courier profiles, high crime areas and others are based on evaluating levels of probability that criminal activity will occur or is occurring.").

indicate that a person is trafficking in illegal narcotics.[154] Each profile characteristic standing alone could describe many "innocent travelers," but police use the factors' confluence to target suspects for further investigation.[155] This practice of inferring crime from facially innocent facts underlies both analog and automated profiling. Thus, the jurisprudence around the drug courier profile is an apt place to begin exploring how courts might consider automated profiling under the Fourth Amendment.

This chapter discusses how federal appellate courts have analyzed the constitutionality of using predetermined crime profiles—particularly the drug courier profile[156]—in police investigations. The Fourth Amendment principles found in these cases provide clues to how courts may begin to assess the constitutionality of automated profiling. They also hint at the challenges courts will face when attempting to apply Fourth Amendment precedent to new digital policing techniques. These challenges will be addressed in Chapter III.

This chapter proceeds in three parts. Part A provides an overview of the drug courier profile's origin, its use by law enforcement, and its acceptance in the courts. Part B analyzes the cases in which the drug courier profile has been relied upon as a basis or partial basis for reasonable suspicion or probable cause. This part discusses the level of

---

[154] United States v. Mendenhall, 446 U.S. 544, 568 (1980).

[155] *See generally, e.g.*, *Sokolow*, 490 U.S. 1.

[156] The drug courier profile is the most well-documented example of a predetermined set of characteristics or behaviors attributed to a particular type of criminal. *See* Wayne R. LaFave, *Controlling Discretion by Administrative Regulations: The Use, Misuse, and Nonuse of Police Rules and Policies in Fourth Amendment Adjudication*, 89 MICH. L. REV. 442, 480 (1990) ("[I]n terms of frequency of use by law enforcement officers and frequency of confrontation by appellate courts, [no profile] matches the drug courier profile."). Cases involving the similarly predetermined "hijacker profile" were also surveyed for this thesis; but the hijacker profile, which was used to target potential hijackers in the 1970s and 1980s, has little bearing on this area of Fourth Amendment law now that the Transportation Safety Administration has broad authority to conduct airport searches. *See* Deborah L. Meyer, *The Spot Program: Hello Racial Profiling, Goodbye Fourth Amendment*, 10 U. MD. L.J. 289, 311–312 (2010).

particularity required for reasonable suspicion and the circumstances in which the profile does and does not meet those standards. It also discusses how courts evaluate law enforcement officers' application of the profile under the Fourth Amendment requirement that each case be considered on its own specific facts. Part C acknowledges the freedom of law enforcement officers to use the profile as a basis for narrowing or focusing their investigations without implicating the Fourth Amendment.

The Drug Courier Profile

The drug courier profile was developed by DEA agents in the 1970s.[157] It is an "amalgam of characteristics"[158] that, according to the DEA, "have tended to distinguish drug couriers from other [airline] passengers."[159] Although the factors that comprise the profile have varied somewhat from case to case,[160] the profile generally includes characteristics such as arrival from or departure to an illegal drug "source city," carrying very little luggage and/or no checked baggage, purchasing airline tickets with cash, appearing nervous, and traveling under an alias.[161] In a typical case, agents approach individuals in airports who—based on the agents' observations and prior knowledge—"match" the profile. Agents ask the suspect to show identification and to answer

[157] *See* Morgan Cloud, *Search and Seizure by the Numbers: The Drug Courier Profile and Judicial Review of Investigative Formulas*, 65 B. U. L. REV. 843, 844 (1985).

[158] *Mendenhall*, 446 U.S. at 568.

[159] United States' Petition for Cert. at 3, United States v. Mendenhall, 446 U.S. 544 (1980). The drug courier profile originated as a way to spot airline passengers who might be drug couriers, so most drug courier profile cases arise from airport stops, but the profile has been applied in other contexts, such as automobile stops, train station stops, and street stops.

[160] *See* Cloud, *supra* note 37, at 879; LaFave, *supra* note 36, at 482; David Cole, *Discretion and Discrimination Reconsidered: A Response to the New Criminal Justice Scholarship*, 87 GEO. L. J. 1059, 1077 (1999); United States v. Sokolow, 831 F.2d 1413, 1418 (9th Cir. 1987), *rev'd*, United States v. Sokolow, 490 U.S. 1 (1989); Grant v. State, 461 A.2d 524, 526 (Md. App. 1983).

[161] United States v. Elmore, 595 F.2d 1036, 1039 n.3 (5th Cir. 1979), *cert denied*, 447 U.S. 910 (1980).

questions in what is usually deemed a "consensual" encounter.[162] "If the agents' suspicions are not eliminated during this exchange," they often move the suspect to another location and/or search the suspect's bags, at which point the interaction typically matures into a Fourth Amendment seizure.[163] When these seizures are challenged on Fourth Amendment grounds, the agents rely upon the matching profile characteristics, along with other observations or information they gained prior to the seizure, to justify the stop. While most drug courier profile cases involve airport stops, the profile's use has expanded beyond airports. Police officers have cited drug courier profile characteristics to justify automobile[164] and pedestrian[165] stops as well.

The Supreme Court has neither prohibited nor explicitly sanctioned the profile's use as a basis for *Terry* stops. In *United States v. Sokolow*,[166] the only Supreme Court case to directly address the profile, the Court held that the reasonable suspicion analysis is not affected by whether officers matched the suspect to a profile.[167] Each case must be decided based upon the particular factors observed and testified to by the officer, regardless of whether those factors were part of a profile. Thus, analyzing the federal appellate courts' assessment of the profile similarly requires a fact-specific, case-by-case analysis.

---

[162] Cloud, *supra* note 37, at 848–49.

[163] *Id.*

[164] *See, e.g.*, United States v. Brugal, 185 F.3d 205, 208–09 (4th Cir. 1999), *opinion vacated*, 209 F.3d 353 (4th Cir. 2000).

[165] *See, e.g.*, United States v. Hawthorne, 982 F.2d 1186, 1187–88 (8th Cir. 1992).

[166] 490 U.S. 1 (1989).

[167] *Id.* at 10.

The Drug Courier Profile and Reasonable Suspicion

Drug courier profile cases usually arise from claims that seizures were not supported by reasonable suspicion. The Fourth Amendment requires brief investigative stops (*Terry* stops) to be supported by specific and articulable facts giving rise to the officer's reasonable inference that "criminal activity 'may be afoot.'"[168] Courts evaluate the reasonableness of officers' inferences based on "the totality of the circumstances—the whole picture."[169] The Supreme Court has cautioned that "[t]he concept of reasonable suspicion . . . is not 'readily, or even usefully, reduced to a neat set of legal rules.'"[170] When officers draw inferences based on the drug courier profile, courts must determine whether the profile factors relied upon, along with any other observations made by or facts known to the officer, were sufficiently particular to the suspect and could lead a reasonable officer to infer that the suspect was engaged or was about to be engaged in criminal activity.[171]

<u>The Particularity Requirement: A Fact-Specific Inquiry</u>

The only clear rule about when the drug courier profile can give rise to reasonable suspicion is that there is no rule.[172] The chief criticism of the profile is that it lacks

[168] *Id.* at 7 (1989) (quoting Terry v. Ohio, 392 U.S. 1, 27 (1968)).

[169] *Id.* at 8 (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).

[170] *Id.* at 7 (quoting Illinois v. Gates, 462 U.S. 213, 232 (1983)).

[171] *Id.* at 7–10.

[172] *See, e.g.*, *Id.* at 10 ("We do not agree with respondent that our analysis is somehow changed by the agents' belief that his behavior was consistent with one of the DEA's 'drug courier profiles.' A court sitting to determine the existence of reasonable suspicion must require the agent to articulate the factors leading to that conclusion, but the fact that these factors may be set forth in a 'profile' does not somehow detract from their evidentiary significance as seen by a trained agent."); United States v. Erwin, 803 F.2d 1505, 1510 (9th Cir. 1986) ("There is no 'litmus test' for reasonable suspicion. Each instance of police conduct must be judged for reasonableness 'in light of the particular circumstances.' . . . The resemblance of facts to the profile does not determine the constitutional validity of a search." (internal citations omitted)).

particularity because it is made up of characteristics that can describe "significant numbers of innocent persons."[173] However, the Supreme Court in *Sokolow* clarified that "innocent behavior will frequently provide the basis for . . . reasonable suspicion." Still, the *Sokolow* Court declined to adopt a rule either sanctioning or prohibiting the profile's use as a basis for reasonable suspicion.[174] Instead, it held that "[a] court sitting to determine the existence of reasonable suspicion must require the agent to articulate the factors leading to that conclusion, but the fact that these factors may be set forth in a 'profile' does not somehow detract from their evidentiary significance as seen by a trained agent."[175] The Court held that "[i]n making a determination of probable cause the relevant inquiry is not whether particular conduct is 'innocent' or 'guilty,' but the degree of suspicion that attaches to particular types of noncriminal acts."[176]

When assessing particularity, courts ask whether the factors giving rise to suspicion, taken together, would sufficiently narrow the population of suspicious individuals, or whether they describe "a very large category of presumably innocent travelers."[177] At least three circuits—the Fourth,[178] Fifth,[179] and D.C.[180] Circuits—have

---

[173] United States v. Sokolow, 490 U.S. 1, 6 (1989); *see also, e.g.*, Reid v. Georgia, 448 U.S. 438, 440–41 (1980); United States v. Saperstein, 723 F.2d 1221, 1228–29 (6th Cir. 1983); United States v. Gooding, 695 F.2d 78, 83 (4th Cir. 1982).

[174] United States v. Sokolow, 490 U.S. 1, 10 (1989) (quoting Illinois v. Gates, 462 U.S. 213, 243–44, n.13 (1983)).

[175] United States v. Sokolow, 490 U.S. 1, 10 (1989). The *Sokolow* Court rejected the district court's attempt to distinguish between facts describing "ongoing criminal activity" and facts describing "personal characteristics," or "probabilistic evidence." *Id.* at 6–10.

[176] *Id.* at 10.

[177] Reid v. Georgia, 448 U.S. 438, 441 (1980).

[178] United States v. Matthews, 25 F.3d 1042, *4 n.1 (4th Cir. 1994) (unpublished) (stating that the fact that a suspect matched the drug courier profile would have been enough to justify a *Terry* stop). *But see* United States v. Gooding, 695 F.2d 78, 83 (4th Cir. 1982) ("[W]e have specifically held that a drug courier profile,

interpreted *Sokolow* as indicating that profile factors, without more, can satisfy this particularity requirement. In *Sokolow*, six of the profile factors, taken together, were sufficient to justify reasonable suspicion. Agents seized Sokolow in the Honolulu airport based on the fact that (1) he paid for his plane tickets in cash; (2) he traveled under an alias; (3) his original destination was Miami, a "source city for illicit drugs;" (4) he had an unusually short stay in Miami; (5) he appeared nervous; and (6) he did not check any luggage.[181] The Supreme Court held that, while "[a]ny one of these factors [was] not by itself proof of any illegal conduct and [was] quite consistent with innocent travel[,] . . . . taken together[,] they amount[ed] to reasonable suspicion."[182] Courts that take a profile-acceptance view of *Sokolow* maintain that while "[s]mall parts of the drug courier profile may not always, standing alone, provide [] reasonable, articulable suspicion[,]"[183] several profile factors taken together may justify a stop.[184]

The Sixth,[185] Seventh,[186] and Eighth[187] Circuits have maintained that the profile, without more, is too general to justify reasonable suspicion, and that it must be combined

---

without more, does not create a reasonable and articulable suspicion."). Note that *Gooding* was decided before *Sokolow*.

179 United States v. Turner, 628 F.2d 461, 462–63 (5th Cir. 1980) (citing United States v. Mendenhall, 446 U.S. 544 (1980)) (holding that *Mendenhall* "implicitly approve[d] the use of the 'drug courier profile'" as a basis for *Terry* stops). *Mendenhall* did not directly address the drug courier profile.

180 United States v. Colyer, 878 F.2d 469, 480–82 (D.C. Cir. 1989) (relying in part on *Sokolow* to find that a drug courier profile applied to Amtrack travelers sufficiently narrowed the number of travelers who came under suspcicion).

181 United States v. Sokolow, 490 U.S. 1, 3 (1989).

182 *Id.* at 9.

183 *See, e.g.*, United States v. Carter, 139 F.3d 424, 432 (4th Cir. 1998) (quoting United States v. Alpert, 816 F.2d 958, 960–61 (4th Cir. 1987)).

184 *See, e.g.*, *Colyer*, 878 F.2d at 480–82.

185 *See, e.g.*, United States v. Cotton, 928 F.2d 405, *1 (6th Cir. 1991) (unpublished).

by other observations to give rise to a lawful *Terry* stop. At least half of the circuit courts[188] have avoided ruling directly on whether the profile alone can justify a *Terry* stop. However, each circuit has found that some combination of the profile factors can justify a stop when accompanied by other observations, such as flight[189] (the suspect flees when approached by authorities); inconsistent or untruthful answers during consensual questioning;[190] an informant tip;[191] a bulge under the suspect's clothing (suggesting a weapon or drugs);[192] or unusual conduct.[193] Observations that alone would not support

---

[186] *See, e.g.*, United States v. Sterling, 909 F.2d 1078, 1083 (7th Cir. 1990).
[187] *See, e.g.*, United States v. Millan, 912 F.2d 1014, 1017 (8th Cir. 1990), *abrogation rec'd by* United States v. Gilbert, 936 F.2d 377 (8th Cir. 1991) (citing United States v. Poitier, 818 F.2d 679, 683 (8th Cir. 1987) ("Although the Supreme Court recently recognized the evidentiary significance of factors that are set forth in a drug courier profile, it did not overrule the oft-cited principle . . . that these factors alone . . . cannot justify a *Terry* stop.").

[188] The First, Second, Third, Ninth, Tenth, and Eleventh Circuits.

[189] *See* United States v. Rodriquez-Sanchez, 23 F.3d 1488, 1493 (9th Cir. 1994); United States v. Brugal, 209 F.3d 353, 360–61 (4th Cir. 2000); United States v. Pope, 561 F.2d 663, 667 (6th Cir. 1977).

[190] *See* United States v. Hardison, 56 F.3d 78 (10th Cir. 1995); United States v. Sterling, 909 F.2d 1078, 1084 (7th Cir. 1990); United States v. Goodwin, 449 F.3d 766, 767–68 (7th Cir. 2006); United States v. Hooper, 935 F.2d 484, 493–94 (2d Cir. 1991); United States v. Hernandez, 854 F.2d 295, 298 (8th Cir. 1988); United States v. Pino, 855 F.2d 357, 363 (6th Cir. 1988), *amended*, 866 F.2d 147 (6th Cir. 1989); United States v. Allen, 842 F.2d 1292 (4th Cir. 1988); United States v. Poitier, 818 F.2d 679, 683 (8th Cir. 1987). *But see* United States v. Urrieta, 520 F.3d 569, 578 (6th Cir. 2008) (finding that a broad profile plus a suspect's untruthful answer about his immigration status did not justify reasonable suspicion that the suspect was a drug courier because such reasoning "opens the door to allowing millions of undocumented immigrants to be detained for further questioning on that basis. To hold that one's illegal presence in this country is a sign of anything more than an immigration violation stretches the Fourth Amendment much too far.").

[191] United States v. Drinkard, 900 F.2d 140, 143 (8th Cir. 1990); United States v. McMurray, 34 F.3d 1405, 1410 (8th Cir. 1994); United States v. Ornelas-Ledesma, 16 F.3d 714, 718–19 (7th Cir. 1994); United States v. Nelson, 42 F.3d 1403 (9th Cir. 1994); United States v. Zukas, 843 F.2d 179, 182–83 (5th Cir. 1988).

[192] *See* United States v. Knox, 839 F.2d 285, 289–90 (6th Cir. 1988); *Allen*, 842 F.2d 1292; United States v. $84,000 U.S. Currency, 717 F.2d 1090, 1092 (7th Cir. 1983); United States v. Smith, 574 F.2d 882, 884–85 (6th Cir. 1978). *But see* United States v. Millan, 912 F.2d 1014, 1017–18 (8th Cir. 1990) (abrogated as to whether a seizure occurred) (finding that the drug courier profile plus a visible bulge did not justify reasonable suspicion).

[193] *See* United States v. Alpert, 816 F.2d 958, 960–61 (4th Cir. 1987).

reasonable suspicion (such as a tip from an unreliable informant[194] or refusal to cooperate with questioning[195]) have been bolstered by the profile. In *United States v. Coggins*,[196] agents stopped a suspected drug courier because he fit the profile and because his travel companions were "recognized individuals involved in illegal activities."[197] The Third Circuit held that while "[m]ere association with a known criminal cannot on its own be a basis for 'reasonable suspicion[,] . . . . when such association is combined with other elements [all of which were profile factors] . . . a reasonable suspicion adequate to support an investigative detention may indeed arise."[198] Courts continue to disagree over whether the drug courier profile alone can justify reasonable suspicion, but *Sokolow* has held open the door for officers to use the profile as a substantial part of the basis for a *Terry* stop.

Courts agree that no set of factors can justify reasonable suspicion if it would subject large numbers of innocent people to *Terry* stops.[199] This is especially true if the

---

[194] *See* United States v. Ornelas-Ledesma, 16 F.3d 714, 718 (7th Cir. 1994) (citing Illinois v. Gates, 462 U.S. 213, 227 (1983)) ("[A]n uncorroborated tip from [] an [unreliable] informant cannot by itself furnish probable cause . . . ."); *Id.* (citing United States v. Hensley, 469 U.S. 221, 232 (1985)) ("[A]n uncorroborated anonymous tip, even when it comes from law enforcement authorities, does not by itself justify a stop.").

[195] *Compare* Florida v. Bostick, 501 U.S. 429, 437 (1991) ("[R]efusal to cooperate, without more, does not furnish the minimal level of objective justification needed for a detention or seizure.") *with* United States v. Goodwin, 449 F.3d 766, 767–68 (2006) (holding that the drug courier profile, combined with Goodwin's refusal to let police search his bag, claiming he had misplaced the key to unlock the bag, justified reasonable suspicion).

[196] 986 F.2d 651 (3d Cir. 1993).

[197] *Coggins*, 986 F.2d at 655.

[198] *Id.*

[199] *See* United States v. Sokolow, 490 U.S. 1, 6 (1989) (emphasizing that the factors justifying reasonable suspicion "did not describe 'significant numbers of innocent persons'"); Reid v. Georgia, 448 U.S. 438, 441 (1980) ("[T]he evidence relied on . . . describe[s] a very large category of presumably innocent travelers, who would be subject to virtualy random seizures were the Court to conclude that as little foundation as there was in this case could justify a seizure."); United States v. Rodriguez, 976 F.2d 592,

factors tend to correlate with one another even in innocent circumstances.[200] The Seventh Circuit criticized[201] a stop on these grounds in *United States v. Ornelas-Ledesma*.[202] Officers pulled over Ornelas-Ledesma because he was driving through California (a state considered a "source state" for drugs) in a 1981 two-door Oldsmobile (a vehicle believed to be one of "drug traffickers' favorites") with another person; he had checked into a motel very late at night with no existing reservation; and he was Hispanic.[203] The court

595–96 (9th Cir. 1992) ("[W]e must not accept . . . [a] profile of suspicious behavior very likely to sweep many ordinary citizens into a generality of suspicious appearance merely on hunch."); United States v. Bravo, 295 F.3d 1002, 1008 (9th Cir. 2002) (citing United States v. Sigmond-Ballesteros, 285 F.3d 1117, 1121 (9th Cir. 2002)) ("[A]n officer[] . . . may not base reasonable suspicion on 'broad profiles which cast suspicion on entire categories of people without any individualized suspicion of the particular person to be stopped.'"); United States v. Montero-Camargo, 208 F.3d 1122, 1129 (9th Cir. 2000) (quoting *Rodriguez*, 976 F.2d at 595–96) ("[W]e have rejected profiles that are 'likely to sweep many ordinary citizens into a generality of suspicious appearance.'"); United States v. Vega-Barvo, 729 F.2d 1341, 1349 (11th Cir. 1984) ("If the profile is overly general, it carries little weight . . . ."); United States v. Manzo-Jurado, 475 F.3d 928, 935 (9th Cir. 2006) ("[T]o establish reasonable suspicion, an officer cannot rely solely on generalizations that, if accepted, would cast suspicion on large segments of the lawabiding [sic.] population."); United States v. Hawthorne, 982 F.2d 1186, 1190 (8th Cir. 1992) (holding that the combined profile factors relied upon by agents "describe[d] a very broad category of predominantly innocent travelers"); United States v. Cotton, 928 F.2d 405 (6th Cir. 1991) (quoting Reid v. Georgia, 448 U.S. 438, 441 (1980) (holding that the facts known to and observed by officers "describe[d] a very large category of presumably innocent travelers who would be subject to virtually random seizures were the Court to conclude that as little foundation as there was in this case could justify a seizure"); United States v. Urrieta, 520 F.3d 569, 576 (6th Cir. 2008) (quoting Reid v. Georgia, 448 U.S. 438, 441 (1980)) ("Standard drug-courier profiles [] are highly problematic because they often 'describe a very large category of presumably innocent travelers, who could be subject to virtually random seizures were the Court to concluded that as little foundation [as the profile] could justify a seizure.'" (emphasis in original)); United States v. Campbell, 843 F.2d 1089, 1094 (8th Cir. 1988) ("[Supreme Court precedent] does not preclude all reliance on courier profile characteristics; it simply indicates that the most general of those characteristics cannot be the sole support for a seizure without more particularized evidence of suspicious activity."); United States v. Brugal, 209 F.3d 353, 370 (4th Cir. 2000) (holding that the factors articulated by officers justified reasonable suspicion because they "eliminate[d] a substantial portion of innocent travelers"); United States v. Colyer, 878 F.2d 469, 482 (D.C. Cir. 1989) (holding that a profile was sufficiently particular when investigations based on the profile "would typically reveal no more than three suspicious reservations on a 400-seat train").

[200] *See* Ornelas-Ledesma, 16 F.3d 714, 716 (7th Cir. 1994).

[201] The stop was ultimately upheld only on the basis of a (false) hit in a criminal database which gave the officers reasonable cause to suspect the defendant of drug trafficking. *Id.* at 717–19.

[202] 16 F.3d 714 (7th Cir. 1994).

[203] *Id.* at 715–17.

dismissed these factors not only because each one was innocent but also because they were all "correlated rather than independent."[204]

> [T]he confluence of these circumstances is pretty innocuous . . . especially since many of the circumstances are correlated . . . . Hispanics are disproportionately concentrated in California, and having on average lower incomes than non-Hispanic Americans are doubtless more likely than other Americans to drive two-door rather than four-door cars, older rather than newer cars, and American rather than foreign cars. They are more likely to drive than to fly and, we imagine, less likely to make reservations in advance at motels, since cheap motels don't advertise much or have 800 numbers. Nothing is more common than for people taking long trips to drive until they're tired and then—often at very odd hours—to check in at the nearest motel, of course without a reservation. And people who drive long distances late at night prefer to have someone with them. Because "suspicious" circumstances . . . are so strongly correlated with each other, were they considered sufficient by themselves to justify a stop the practical consequences would be that a very large population of all Hispanic Americans would be vulnerable to being stopped on suspicion of drug trafficking. Hispanics would be second-class citizens in the eyes of the police.[205]

Not all courts have found this prohibition of overly broad profiles to be incompatible with exclusive reliance on the drug courier profile. The Fourth[206] and D.C.[207] Circuits have accepted the profile as sufficient to justify reasonable suspicion on the grounds that the profile factors significantly narrowed the field of potential suspects. In *United States v.*

---

[204] *Id.* at 717.

[205] *Id.* at 716–17.

[206] United States v. Brugal, 209 F.3d 353, 370 (4th Cir. 2000) (holding that the factors articulated by officers justified reasonable suspicion because they "eliminate[d] a substantial portion of innocent travelers").

[207] United States v. Colyer, 878 F.2d 469, 482 (D.C. Cir. 1989) (holding that a profile was sufficiently particular when investigations based on the profile "would typically reveal no more than three suspicious reservations on a 400-seat train").

Colyer,[208] the D.C. Circuit held that a profile used to stop an Amtrak customer was sufficiently particular when an Amtrak agent testified that investigations based on the profile "would typically reveal no more than three suspicious reservations on a 400-seat train."[209] The quantitative specificity of *Colyer* is anomalous. Other courts simply found that the profile "did not describe 'significant numbers of innocent persons.'"[210] Or that it "eliminate[d] a substantial portion of innocent travelers."[211]

An officer's training and experience can give extra weight to inferences based on profiles developed by law enforcement.[212] The Fourth Amendment reasonable suspicion standard allows officers to reasonably infer criminal conduct from facially innocent observations in light of the officers' training and experience.[213] In *United States v. Price*,[214] the Second Circuit held that "it is appropriate for a court to take into account characteristics enumerated in the profile, which represents 'a kind of institutional

---

[208] 878 F.2d 469 (D.C. Cir. 1989).

[209] *Colyer*, 878 F.2d at 482.

[210] *Sokolow*, 490 U.S. at 6.

[211] *Brugal*, 209 F.3d at 360.

[212] *Colyer*, 878 F.2d at 479 (giving weight to the fact that "rather than mechanically matching appellant's [airline] reservation with a profile, [the agent] selected those manifests which, on the basis of his training and experience, appeared suspicious"); United States v. Price, 599 F.2d 494, 502 (2d Cir. 1979) (quoting United States v. Rico, 594 F.2d 320, 326 (2d Cir. 1979)) ("[I]t is appropriate for a court to take into account characteristics enumerated in the profile, which represents 'a kind of institutional expertness' derived from the cumulative experience of DEA surveillance teams."). *But see* United States v. Taylor, 917 F.2d 1402, 1408 (6th Cir. 1990) (expressing doubt about the officer's ability to draw inferences based on profile factors when the officer "had *little* on-the-job experience with [the profile]"); United States v. Wilson, 953 F.2d 116, 124 (4th Cir. 1991) (quoting United States v. Gooding, 695 F.2d 78, 82 (4th Cir. 1982)) ("[A]lthough trained law enforcement officers may be able to perceive suspicious conduct not visible to an untrained observer, 'any such special meaning must be articulated to the courts and its reasonableness as a basis for seizure assessed independently of the police officers' subjective assertions . . . .'").

[213] *See Sokolow* at 9–10.

[214] 599 F.2d 494 (2d Cir. 1979).

expertness' derived from the cumulative experience of DEA surveillance teams."[215] However, a *lack* of training or familiarity with the profile can work against the officer applying it.[216] In *United States v. Taylor*,[217] the Sixth Circuit invalidated a stop in part because the court doubted the officer's ability to make profile-based inferences when he had little training or experience with the profile.[218] Moreover, the Fourth Circuit has cautioned that any special meaning interpreted by officers "must be articulated to the courts."[219] Officers who are versed in the drug courier profile may infer special, articulable meaning from permutations of its factors, but they cannot prevail simply by invoking the profile.

The *Terry* Stop Exigency Requirement

All investigative stops must be justified by temporal exigency. Officers conducting *Terry* stops "must have reasonable suspicion [that] the individual [being stopped] *has, or is about to have, committed a crime*.[220] The authority of law enforcement to make stops and searches without first obtaining warrants is rooted in the need to apprehend individuals before they can flee, endanger others, or otherwise break the law.[221] Thus, conformance with a profile cannot justify an investigative stop if the

[215] *Id.* at 502.

[216] *See* United States v. Taylor, 917 F.2d 1402, 1408 (6th Cir. 1990) (expressing doubt about the officer's ability to draw inferences based on profile factors when the officer "had *little* on-the-job experience with [the profile]").

[217] 917 F.2d 1402 (6th Cir. 1990).

[218] *Id.* at 1408.

[219] *Gooding*, 695 F.2d at 82; *Wilson*, 953 F.2d at 124.

[220] United States v. Manzo-Jurado, 457 F.3d 928, 934 (9th Cir. 2006) (citing United States v. Brigoni-Ponce, 422 U.S. 873, 884 (1975)) (emphasis added).

[221] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 22 (1968)

observed factors do not tend to indicate that a person has committed or is about to commit a crime. In *United States v. Mendez*,[222] the Ninth Circuit held that a tattoo indicating a certain gang affiliation could not justify a stop because, although it

> might arouse suspicion that [Mendez] was involved in criminal activity at some point in the past and might lead a reasonable officer to suspect that he may become involved in such activity at some point in the future, it does not support a reasonable inference 'that criminal activity may *be afoot*' at the time of the stop or that Mendez might commit any *particular offense* now or in the future.[223]

The Seventh Circuit has upheld the drug courier profile, without more, as justification for a stop when police had an exigent need to interrupt a potential imminent drug deal.[224] In *United States v. Goodwin*,[225] police officers boarded a train in order to question a passenger who was flagged as fitting several drug courier profile characteristics—in particular, a last-minute one-way ticket purchased with cash.[226] The court wrote that

> [i]f the defendant had bought his ticket a week in advance and the police had known then that he fit the profile of a drug courier, they could have arranged for Dusty (the sniffer dog) to be at Union Station when the train was scheduled to depart [thus avoiding the need to board the train]. But because the defendant bought his ticket only an hour before the scheduled departure, the police had until then no ground for suspicion. Their only options at that point were to risk causing the defendant to miss his train or abandon the investigation. To say that it was unreasonable for them to choose the former course of action would make

[222] 467 F.3d 1162 (9th Cir. 2007).

[223] *Id.* at 1169 (quoting Terry v. Ohio, 392 U.S. 1, 30 (1968)) (alterations in original).

[224] United States v. Goodwin, 449 F.3d 766, 771 (7th Cir. 2006).

[225] 449 F.3d 766 (7th Cir. 2006).

[226] *Id.* at 767–68.

> last-minute ticket purchases a foolproof way for drug couriers to frustrate profiling.

Goodwin and *Manzo-Jurado* demonstrate that the reasonableness of suspicion derives not only from the soundness of officers' inferences but also from the perceived exigency of the stop. However, there is little discussion of exigency in the drug courier profile cases, because the profile rests on an assumption that its factors indicate an *imminent* (if not already carried out) drug deal.

<u>The requirement for Fourth Amendment review on a case-by-case basis</u>

The use of a profile does not obviate each court's requirement to engage in a fact-specific reasonable suspicion analysis.[227] As the Supreme Court has noted: "There is no 'litmus test' for reasonable suspicion. Each instance of police conduct must be judged for reasonableness 'in light of the particular circumstances.'"[228] This standard precludes officers from relying on "mere rote citations of factors which were held, in some past situations, to have generated reasonable suspicion."[229] Thus, "the DEA drug courier profile has [] *not* received a blanket stamp of approval" because such a "stamp" would contravene Fourth Amendment review.[230] The fact that a number of coinciding profile factors justified reasonable suspicion in one case does not mean that the same factors create reasonable suspicion in a different case.[231]

---

[227] United States v. Price, 599 F.2d 494, 502 (2d Cir. 1979).

[228] United States v. Erwin, 803 F.2d 1505, 1510 (9th Cir. 1986) (quoting Terry v. Ohio, 392 U.S. 1, 21 (1968)).

[229] United States v. Rodriguez, 976 F.2d 592, 594 (9th Cir. 1992).

[230] United States v. Saperstein, 723 F.2d 1221, 1227–28 (6th Cir. 1983).

[231] *See Rodriguez*, 976 F.2d at 594 ("[W]e must be watchful for mere rote citations of factors which were held, in some past situations, to have generated reasonable suspicion, leading us to defer to the supervening wisdom of a case not now before us."). *Id.* at 595–96 ("[W]e must not accept what has come to appear to be a prefabricated or recycled profile of suspicious behavior . . . . This is required by the [F]ourth

Despite the requirement of a fact-specific inquiry, courts give considerable deference to officers' knowledge and experience, which allows officers to make inferences that would not be considered reasonable for a layperson.[232] In *United States v. Price*,[233] the Second Circuit upheld a *Terry* stop based on profile factors observed by an experienced DEA agent.[234] The Court found it relevant that "[Agent] Whitmore ha[d] been with the DEA since its inception in 1973[,] . . . had been assigned to monitor flights [in the airport] for two years[, and] . . . . had participated on several occasions in stops of passengers who were in fact carrying heroin."[235] Although courts cannot simply accept the drug courier profile as a stand-in for reasonable inferences, even skeptical judges have acknowledged that there is some value in the profile as a distillation of DEA agents' collective experience observing drug couriers. The *Price* court articulated this balance:

> The reasonableness of a stop must ultimately be determined solely by the reviewing court, and that court cannot be bound by a profile developed by the law enforcement officers whose actions are being reviewed. However, it is appropriate for a court to take into account characteristics enumerated in the profile, which represents "a kind of institutional expertness" derived from the cumulative experience of DEA surveillance teams.[236]

The *Price* court thus suggested that some deference is due not only to the experience of the officer applying the profile and drawing inferences from it but also to the collective

---

[A]mendment. The opinions of this court have put the nomenclature of reasonable suspicion into the public domain. We must not allow ourselves to be seduced by the reassuring familiarity of its echo.").

[232] *See* Ornelas, 517 U.S. 690, 699 (1996); United States v. Price, 599 F.2d 494, 501 (2d Cir. 1979) ("The circumstances surrounding the stop . . . . 'are to be viewed through the eyes of a reasonable and cautious police officer on the scene, guided by his experience and training.'").

[233] 599 F.2d 494 (2d Cir. 1979).

[234] *Id.* at 501.

[235] *Id.*

[236] *Price*, 599 F.2d at 502 n. 10.

"institutional expertness" of the DEA agents who developed the profile in the first place.[237]

When evaluating reasonable suspicion founded on a profile, courts require officers to testify to the specific profile characteristics giving rise to suspicion.[238] The meaning of these factors to the officer in light of his or her training and experience must also be articulated.[239] In *United States v. Wilson*,[240] the Fourth Circuit did not find reasonable suspicion because the officer failed to articulate the "special meaning" of a bulge observed in Wilson's pocket in conjunction with drug courier profile factors.[241] The court held that it could not find reasonable suspicion because it was unable to assess the officer's inferences without testimony as to his reasoning.[242] The *Wilson* court contrasted these facts with those in *United States v. Aguilar*,[243] which were substantially similar except that the officer in *Aguilar* testified that he "had observed other passengers' [sic] with bulges at the ankles and that on each occasion it turned out that the bulge was a

---

[237] *Id.*

[238] *See* United States v. Wilson, 953 F.2d 116, 124 (4th Cir. 1991) (quoting United States v. Gooding, 695 F.2d 78, 82 (4th Cir. 1982)) ("[A]lthough trained law enforcement officers may be able to perceive suspicious conduct not visible to an untrained observer, 'any such specific meaning must be articulated to the courts and its reasonableness as a basis for seizure assessed independently of the police officers' subjective assertions . . . .'"); *see also* United States v. Bell, 464 F.2d 667, 669–72 (2d Cir. 1972) (requiring agents to testify to the factors comprising a confidential "hijacker profile" but allowing them to bar the public and defendant (but not the defendant's counsel) based upon "the compelling urgency of protecting the confidentiality of the profile which has been devised as a method to reduce the threat of hijacking").

[239] United States v. Wilson, 953 F.2d 116, 124 (4th Cir. 1991) (quoting United States v. Gooding, 695 F.2d 78, 82 (4th Cir. 1982)) ("[A]lthough trained law enforcement officers may be able to perceive suspicious conduct not visible to an untrained observer, 'any such specific meaning must be articulated to the courts and its reasonableness as a basis for seizure assessed independently of the police officers' subjective assertions . . . .'").

[240] 953 F.2d 116 (4th Cir. 1991).

[241] *Id.* at 124.

[242] *Id.*

[243] 825 F.2d 39 (4th Cir. 1987).

packet of illegal drugs."[244] Courts give considerable weight to officers' interpretation of facially innocent profile factors, but innocent facts alone are insufficient if their "special meaning" cannot be articulated.

Even in the context of a profile, some courts have refused to consider individual characteristics that are too broad to be probative of criminal activity.[245] In fact, the Ninth Circuit has held that profile factors whose probative value is too low to be reasonably relied upon must not be considered.[246] In *United States v. Montero-Camargo*,[247] the Ninth Circuit found that officers had reasonable suspicion to stop Montero-Camargo but that "some of the factors on which the district court relied [were] not relevant . . . to the reasonable suspicion analysis."[248] The court found that Montero-Camargo's Hispanic appearance was not reasonably probative of undocumented status, since a substantial number of innocent people shared that specific characteristic:[249]

> Where, as here, the majority (or any substantial number) of people share a specific characteristic[,] that characteristic is of little or no probative value in such a particularized and context-specific analysis. . . . The likelihood that in an area in which the majority—or even a substantial part—of the population is Hispanic, any given person of Hispanic

---

[244] *Wilson*, 953 F.2d at 124 (quoting *Aguilar*, 825 F.2d at 41) (alterations in original).

[245] *See* United States v. Montero-Camargo, 208 F.3d 1122, 1131–32 (9th Cir. 2000); United States v. Manzo-Jurado, 457 F.3d 928, 937 (9th Cir. 2006) ("The agents' observation that the group members appeared out of place at the football game has no relevance to establishing reasonable suspicion because nothing suggests such behavior indicates an individual's illegal status in this country. Observations so ambiguous that they bear little relationship to any sort of criminality have low, if any, probity toward finding reasonable suspicion.").

[246] *Montero-Camargo*, 208 F.3d at 1132 ("As we have previously held, factors that have such low probative value that no reasonable officer would have relied on them to make an investigative stop must be disregarded as a matter of law.").

[247] 208 F.3d 1122 (9th Cir. 2000).

[248] *Id.* at 1131.

[249] *Id.* at 1131–32.

> ancestry is in fact an alien, let alone an illegal alien, is not high enough to make Hispanic appearance a relevant factor in the reasonable suspicion calculus.[250]

The Fourth Circuit has similarly refused to give any weight to the fact that a suspect was traveling to or from a narcotics "source city" when this factor has appeared in conjunction with other drug courier profile factors.[251] The Fourth Circuit in *United States v. Carter*[252] wrote that "the idea of law enforcement authorities conducting investigations based on the air travel of a suspect is dubious at best, particularly when the destinations are in fairly reasonable proximity to one another."[253] However, these assertions are rare. Most courts have considered each factor and its relative probity in light of all of the circumstances.

Despite a strong jurisprudential abhorrence for "litmus test[s][,]"[254] the Second Circuit may have left some room for a more objectively reliable profile to serve as a proxy for reasonable suspicion. In 1972, the Second Circuit decided *United States v. Bell*,[255] one of many cases in that decade involving the Federal Aviation Administration's airline "hijacker profile."[256] The FAA used the profile to screen passengers, based on their reservations, for further investigation.[257] The *Bell* court held that the hijacker profile

---

250 *Id.*

251 *See* United States v. Carter, 139 F.3d 424, 432 (4th Cir. 1998).

252 139 F.3d 424 (4th Cir. 1998).

253 *Id.* at 432.

254 United States v. Erwin, 803 F.2d 1505, 1510 (9th Cir. 1986) (quoting Terry v. Ohio, 392 U.S. 1, 21 (1968)).

255 464 F.2d 667 (2d Cir. 1972).

256 *Id.* at 669–70.

257 *Id.*

satisfied reasonable suspicion because it was "constructed based on scientific, sociological and psychological data" and could be "readily and objectively employed by [a] ticket seller without requiring any subjective interpolation."[258] Although the *Bell* court found that the agents did not rely on the profile alone, its analysis strayed from strict adherence to the Fourth Amendment requirement for an independent inquiry into the facts in each case.[259] *Bell* may be anomalous, but its unequivocal deference to a data-driven, empirically reliable profile is noteworthy, particularly in light of courts' skepticism of the drug courier profile's reliability, which will be addressed in the next subsection.

<u>Courts' Skepticism Toward the Profile</u>

At least five circuit courts[260] have expressed doubts about the reliability of the drug courier profile and about law enforcement officers' objective application of the profile. Some simply find it unhelpful, calling it a "protean concept,"[261] a "shopworn amalgam,"[262] and "highly problematic"[263] because it can describe "a very large category of presumably innocent travelers."[264] Others have expressed wariness at basing

---

[258] *Id.* and 670. The court also considered the fact that "the profile, according to sizeable sampling, select[ed] less than 1 % of the passengers as possible hijackers." *Id.*

[259] *Id.*

[260] The Fourth, Sixth, Eighth, Ninth, and Eleventh Circuits.

[261] United States v. Wilson, 953 F.2d 116, 124 (4th Cir. 1991).

[262] United States v. Puglisi, 723 F.2d 779, 789 (11th Cir. 1984).

[263] United States v. Urrieta, 520 F.3d 569, 576 (6th Cir. 2008).

[264] *Id. See also* United States v. Drinkard, 900 F.2d 140, 143 (8th Cir. 1990).

reasonable suspicion on law enforcement officers' application of a profile created by law enforcement.[265]

Perhaps chief among these concerns is the profile's "malleable" nature.[266] In his dissenting opinion in *Sokolow*, Justice Thurgood Marshall criticized the profile's "chameleon-like way of adapting to any particular set of observations."[267] The Sixth Circuit in *United States v. Respress*[268] enumerated some of the profile's inconsistencies from case to case:

> A quick survey of various cases involving drug courier profiles can easily establish how malleable the factors relied upon are. For instance, though Officer Jones says he found it suspicious that Respress had no carry-on luggage, in *United States v. Sokolow,* 490 U.S. 1, 5, 109 S.Ct. 1581, 1584, 104 L.Ed.2d 1 (1989), what the officer found suspicious is that the alleged courier *did* have carry-on luggage. Similarly, Jones found it suspicious that Respress was the second to last passenger to deplane, while the defendant in *United States v. Moore,* 675 F.2d 802, 803 (6th Cir. 1982), created suspicion by being first to deplane. Additionally, the cases reveal quite a large number of "drug source cities," though the source city in this case (Ontario, California) is not often mentioned.[269]

The Ninth Circuit in *Rodriguez*[270] expressed similar skepticism toward the *consistency* with which the same profile factors were coinciding in multiple different cases:

> We note, initially, that this is not the first time Border Patrol agents have tendered a similar profile to this court as evidence of the existence of reasonable suspicion. In fact,

[265] *See Drinkard*, 900 F.2d at 143.

[266] United States v. Respress, 9 F.3d 483, 490 (6th Cir. 1993).

[267] United States v. Sokolow, 490 U.S. 1, 13 (1989) (Marshall, J., dissenting).

[268] 9 F.3d 483 (6th Cir. 1993).

[269] *Id.* at 490 (internal citations omitted).

[270] United States v. Rodriguez, 976 F.2d 592 (9th Cir. 1992).

> this profile is so familiar, down to the very verbiage chosen to describe the suspect, that an inquiring mind may wonder about the recurrence of such fortunate parallelism in the experiences of the arresting agents.[271]

The Sixth Circuit has warned that the profile's malleability makes it an attractive pretext for race-based stops.[272] The *Respress* court wrote that "[w]hen courts give significant weight to an officer's reliance on such [general] descriptions, it becomes easy for the profile to be used as a pretext for a relevant factor the officer does not wish to articulate, namely a suspect's race."[273]

Critics of the drug courier profile assert that it allows police officers too much discretion[274] *and* that it is too "mechanistic"[275]—two criticisms that appear to contradict each other.[276] Concerns about discretion stem from the profile's breadth and malleability—the profile allows officers to stop individuals based on factors wholly capable of an innocent explanation; it is capable of "adapting to any particular set of observations";[277] and it does not "predetermine just what combination of suspicious factors must exist for a lawful stop."[278] This can lead to arbitrary stops.[279] On the other

[271] *Id.* at 595.

[272] *See Respress*, 9 F.3d at 490; United States v. Jennings, 985 F.2d 562 (6th Cir. 1993).

[273] *Respress*, 9 F.3d at 490.

[274] *See, e.g.*, United States v. Manzo-Jurado, 457 F.3d 928, 934–35 (9th Cir. 2006); Wayne R. LaFave, *Controlling Discretion by Administrative Regulations: The Use, Misuse, and Nonuse of Police Rules and Policies in Fourth Amendment Adjudication*, 89 MICH. L. REV. 442, 480–83 (1990) (citing United States v. Sokolow, 490 U.S. 1, 13 (1989) (Marshall, J., dissenting)).

[275] *See, e.g.*, United States v. Sokolow, 490 U.S. 1, 13 (1989) (Marshall, J., dissenting).

[276] *See* LaFave, *supra* note 36, at 482.

[277] *Id.* (citing *Sokolow*, 490 U.S. at 13).

[278] *Id.*

[279] *Id.*

hand, some of the profile's critics warn that it is too formulaic and should not override officers' common sense. This view actually champions officer discretion, not in the form of arbitrary stops but in the form of more careful and nuanced deliberation.[280] Justice Marshall wrote that

> law enforcement officer's mechanistic application of a formula of personal and behavioral traits in deciding whom to detain can only dull the officer's ability and determination to make sensitive and fact-specific inferences "in light of his experience," particularly in ambiguous or borderline cases. Reflexive reliance on a profile of drug courier characteristics runs a far greater risk than does ordinary, case-by-case police work of subjecting the profile's "chameleon-like way of adapting to any particular set of observations."[281]

Ultimately, courts generally agree that "[w]hile [the profile] may be helpful in some situations, it detracts from the proper test . . . : whether specific, articulable facts *in this case*, considered on the totality of the circumstances, indicate reasonable suspicion."[282]

The profile as an investigative tool

With a few exceptions, courts have avoided holding that the drug courier profile alone can justify reasonable suspicion. For the most part, they haven't been forced to make this decision. Law enforcement officers can often articulate observations or facts other than the profile that contributed to reasonable suspicion. In most cases, the profile serves as a screening mechanism, helping officers target certain individuals to watch more closely, to follow, or to consensually question, before the encounter becomes a Fourth Amendment stop. Courts agree that "[t]he profile is a lawful starting point for police

---

[280] *See Sokolow*, 490 U.S. at 13 (Marshall, J., dissenting).

[281] *Id.*

[282] United States v. Puglisi, 723 F.2d 779, 789 (11th Cir. 1984) (citing Berry, 670 F.2d 583, 600 (1982)).

investigations."[283] For example, the First Circuit has described the profile as "designed to guide the focus of the agents' observations," adding that "only when the characteristics are combined in a suspicious manner, or lead the agents to observe independently suspicious conduct, is official intrusion warranted."[284] Police interactions that fall short of a seizure do not implicate the Fourth Amendment, and there are no Constitutional limits on what factors or information officers can rely on to focus their investigations.[285] Thus, law enforcement can largely avoid Constitutional scrutiny by using, or appearing to use, profiles merely as a "starting point" to "focus" investigations.[286]

Conclusion

This chapter has analyzed federal appellate jurisprudence of predetermined profiles—particularly the drug courier profile—and their use in investigative stops. Several principals have emerged from this body of law: (1) There is no talismanic acceptance in the courts of the drug courier profile, or any other profile, as an indication of reasonable suspicion, and the establishment of such a "litmus test" would likely violate the courts' responsibility to adjudicate each Fourth Amendment case on its own facts; (2) for a

---

[283] United States v. Respress, 9 F.3d 483, 493 (6th Cir. 1993) (citing United States v. Sokolow, 490 U.S. 1 (1989)) *see also* United States v. Saucedo, 226 F.3d 782, 789 (6th Cir. 2000) (holding that a tip constituting a "mere hunch" could not justify a *Terry* stop but could be investigated by means falling short of a *Terry* stop); United States v. Goodwin, 449 F.3d 766, 767 (7th Cir. 2006) ("[T]hough not to establish probable cause or even reasonable suspicion to believe that someone who fits the profile *is* a drug courier[,] [t]he profile is used merely as a basis for deciding whom to investigate further."); United States v. Manchester, 711 F.2d 458, 461 (1st Cir. 1983) (quoting United States v. Berryman, 706 F.2d 1241, 1247 (1st Cir. 1983)) ("[T]he profile is simply a collage of otherwise innocent characteristics designed to guide the focus of the agents' observations, and only when the characteristics are combined in a suspicious manner, or lead the agents to observe independently suspicious conduct, is official intrusion warranted.").

[284] *Manchester*, 711 F.2d at 461 (quoting United States v. Berryman, 706 F.2d 1241, 1247 (1st Cir. 1983)).

[285] *See* Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 Harv. L. & Pol'y Rev. 15, 17 (2016) ("Unlike arrests or wiretaps, the decision to focus police attention on a particular person, without more, is unlikely to be considered a Fourth Amendment 'search.' Thus, the police are not required to demonstrate 'probable cause' or 'reasonable suspicion'—the usual standards of individualized suspicion—to decide whether to conduct surveillance on an individual.").

[286] *See supra* notes 131–32 and accompanying text.

profile to justify reasonable suspicion, it must sufficiently narrow the pool of potential suspects such that it would not cast general suspicion upon "a very large category of presumably innocent [individuals][]"[287]; (3) an officer's training and experience can allow her to infer criminal activity from facially innocent factors, but a lack of experience with a profile or the inability to articulate these inferences can militate against reasonableness; (4) all *Terry* stops, profile-based or not, must be justified by some exigency; (5) courts are generally wary of the drug courier profile's malleability, the lack of proof of its statistical reliability, its mechanistic application by police officers, and its tendency to give officers too much discretion as to whom to stop; and (6) the profile's use as an investigative "starting point" may obviate Fourth Amendment scrutiny altogether. The following chapter will discuss how these principals apply to automated profiling tools and practice.

[287] Reid v. Georgia, 448 U.S. 438, 441 (1980).

CHAPTER 3: AUTOMATED PROFILING

Introduction

The previous chapter discussed how federal appellate courts have treated analog profiles—in particular the drug courier profile—when they are used to justify investigative stops. The Fourth-Amendment constitutionality of a profile-based investigative stop generally depends upon three considerations: (1) the specific profile factors relied upon to justify reasonable suspicion; (2) the role and robustness of the officer's experience and knowledge; and (3) the ability of the applied profile to narrow the pool of "suspicious" individuals. Moreover, exigency is a prerequisite for any warrantless Fourth Amendment seizure.

As discussed in Chapter I, automated profiling can be analogized to analog profiles, such as the drug courier profile. Both automated and analog profiles rely on observed relationships between facially innocent characteristics and criminal conduct. A predictive algorithm essentially creates a profile made up of factors that it thinks are statistically associated with crime. The more risk factors an individual has, the better she fits this profile, and the more likely she is to receive a high threat score. However, the automated nature of automated profiling makes it unlike any investigative practice that courts have considered under the Fourth Amendment reasonable suspicion standard.

Predictive policing algorithms—including automated profiles—"mine . . . huge amounts of [data] . . . in ways that the human brain cannot."[288] Instead of relying on police commanders or analysts to interpret data and decipher trends, automated profiling uses "machine learning."[289] Machine learning allows computers to analyze big data sets for patterns and relationships, and to use those patterns as rules for making predictions.[290] Thus, predictive policing algorithms are programmed to make their own judgments about how to analyze data and what factors to focus on when predicting future crime.[291] The introduction of machine learning and automation into the investigative process will complicate the reasonable suspicion analysis courts have applied to analog profiling. This chapter will analyze the ways in which automation will present new challenges to courts attempting to conduct reasonable suspicion analyses.

This chapter proceeds in four sections. Section A will address how automation might confound inquiries into the specific factors underlying the decision to stop an individual. Section B will address the role (or lack thereof) of the officer's experience and knowledge in making an automated prediction-based stop. Section C will discuss the ability of automated profiles to narrow the pool of suspicious individuals and to avoid subjecting large numbers of innocent individuals to arbitrary seizures. Finally, section D

[288] New York Times, Cities for Tomorrow, *Data Mining and the Modern City* (2015), http://nytcitiesfortomorrow.com/gallery/cities-for-tomorrow-2016/2015-videos/1517.

[289] *See* PredPol, *5 Common Myths About Predictive Policing* (Oct. 12, 2014), http://www.predpol.com/5-common-myths-predictive-policing-predpol/.

[290] *See* Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 88–90 (2014); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 796 (2015) ("[B]ig data relies upon supercomputing and machine learning or artificial intelligence tools and, therefore, by its very definition, big data exceeds the ability of human capacities to make sense of the 'big data' without the assistance of algorithmic tools and other computer-enabled devices.").

[291] *See* Alexander H. Kipperman, Note and Comment, *Frisky Business: Mitigating Predictive Crime Software's Facilitation of Unlawful Stop and Frisks*, 24 TEMP. POL. & CIV. RTS. L. REV. 215, 220 (2014) (describing how PredPol works).

will discuss the use of automated profiling in police actions that do not fall under the Fourth Amendment's protections. Section D will also discuss exigency issues that might arise with the use of automated profiling.

Automated Predictions and the Fact-Specific Reasonable Suspicion Inquiry

Courts are unlikely to give "a blanket stamp of approval" to the use of automated predictions as justifications for *Terry* stops.[292] Under the Fourth Amendment, courts are required to engage in a fact-specific reasonable suspicion analysis in each case.[293] The Supreme Court held in *Terry* that "[t]here is no 'litmus test' for reasonable suspicion."[294] The reviewing court "cannot be bound by a profile."[295] This standard has precluded courts from giving talismanic significance to the drug courier profile,[296] and there is no precedent suggesting that automated predictions would be evaluated differently. Instead, police officers relying on automated predictions to perform investigative seizures would likely be required to testify to the individual factors considered in making the prediction.

Testifying to the reasoning of a machine-learning algorithm might be challenging for police officers. The automated nature of automated predictions de-emphasizes the police officer's experience, knowledge, and observations—the crux of traditional Fourth

[292] United States v. Saperstein, 723 F.2d 1221, 1227–28 (6th Cir. 1983). As Andrew Guthrie Ferguson has argued, courts are unlikely to accept an automated prediction standing alone as a justification for reasonable suspicion. Ferguson (2012), *supra* note 120, at 305. As in many of the drug courier profile cases, the predictions are more likely to be relied upon in conjunction with other observations or facts. However, this does not obviate the need to justify the reasonableness of relying on the prediction as a part of the totality of the circumstances.

[293] United States v. Price, 599 F.2d 494, 502 (2d Cir. 1979).

[294] United States v. Erwin, 803 F.2d 1505, 1510 (9th Cir. 1986) (quoting Terry v. Ohio, 392 U.S. 1, 21 (1968)).

[295] *Price*, 599 F.2d at 502 n. 10.

[296] *See Saperstein*, 723 F.2d at 1227–28; *Price*, 599 F.2d at 502; *Erwin*, 803 F.2d at 1510; United States v. Rodriguez, 976 F.2d 592, 594 (9th Cir. 1992).

Amendment reasonable suspicion inquiry.[297] Predictive policing algorithms use machine learning to process large data sets "in ways that the human brain cannot."[298] The algorithms are typically created by private companies and sold to police departments, and the data they process can come from any number of sources.[299] Thus, the police officer who sees and acts upon an automated prediction will not necessarily know each underlying fact that led the computer to infer that an individual was likely to commit a crime. A mere showing that the predictive software is reliable and accurate cannot satisfy the reasonableness inquiry. Since the prediction is based on underlying facts, the Fourth Amendment inquiry currently requires that the officer testify to those facts.

Moreover, it may not be enough simply to recite the factors that a predictive model generally considers. Such a recitation would not necessarily represent the factors that weighed into a particular prediction. For example, police in Morris County, New Jersey, used five variables to geographically predict burglaries: (1) "past burglaries"; (2) "the residential location of individuals arrested for theft of burglary between 2009 and 2011"; (3) "the proximity to major highways"; (4) "the geographic concentration of males between the ages of 16 and 24"; and (5) "the location of apartment complexes and hotels."[300] However, a prediction based on this risk model would not necessarily indicate that every factor on this list was present. In the drug courier profile context, courts have

[297] *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 21–22 (1968); United States v. Sokolow, 490 U.S. 1, 8–10 (1989); United States v. Montoya de Hernandez, 473 U.S. 531, 542 (1985).

[298] New York Times, Cities for Tomorrow, *Data Mining and the Modern City* (2015), http://nytcitiesfortomorrow.com/gallery/cities-for-tomorrow-2016/2015-videos/1517; Hu, *supra* note 290, at 796.

[299] *See, e.g.*, HunchLab, Features, https://www.hunchlab.com/features/.

[300] JEFFREY S. PAUL & THOMAS M. JOINER, INTEGRATION OF CENTRALIZED INTELLIGENCE WITH GEOGRAPHIC INFORMATION SYSTEMS: A COUNTYWIDE INITIATIVE, GEOGRAPHY & PUB. SAFETY 7 (2011).

held that some factors or combinations of factors constituting *part* of a profile were too general to justify reasonable suspicion.[301] Fourth Amendment reasonable suspicion jurisprudence suggests that officers must testify to the specific factors bearing on each individual prediction. At the very least, courts should ask whether the predictive model at issue required a certain number of the factors to be present before labeling an individual as at-risk of committing a crime.

The requirement for officer testimony may conflict with police departments' and software companies' desire to maintain the secrecy of proprietary algorithms. However, there is precedent for allowing officers to exclude the public and opposing parties from hearing this testimony. In *United States v. Bell*,[302] the Second Circuit allowed police officers to testify to the "hijacker profile" in a closed courtroom, "limited to counsel."[303] The court found it "not only highly desirable but essential, if the profile system is to continue, that [the hijacker profile] be kept confidential."[304] Similar allowances are plausible in the automated profiling context. The policy implications of this secrecy will be addressed in Chapter Four.

Automated Inferences and the Role of the Officer's Experience

The current reasonable-suspicion inquiry focuses on the experience and knowledge of the police officer.[305] Courts ask what facts the officer knew or observed at the time of the seizure and how the officer's training and experience informed her

[301] *See supra* note 183 and accompanying text.

[302] 464 F.2d 667(2d Cir. 1972).

[303] *Id.* at 669–70.

[304] *Id.* at 670.

[305] *See supra* notes 212–19 and accompanying text.

inferences.[306] This inquiry is at odds with automated predictions. Automated predictions are based on facts known to a computer, and the knowledge the computer has "learned" from all of the data it has processed.[307] The point of using automated decision-making systems is that they can "learn" and process more information more efficiently than a human police officer.[308] This raises questions about how, if at all, a police officer's experience and training should factor into a reasonable suspicion analysis arising from an automated prediction. When an officer takes some action based on a computer's probabilistic prediction, is the officer making an inference, or is the officer simply responding to a computer's inference?

The use of automated predictions involves at least some measure of substituting a computer's judgment for the officer's judgment. The doctrine of reasonable suspicion rests on the assumption that officers must make quick but reasonable decisions based upon what they observe, what they know, and what their past experience tells them about a situation. But what happens when a computer purports to know something the officer doesn't? Under Fourth Amendment review of investigative seizures, an officer is not entitled to inferences that she cannot articulate.[309] If courts are to apply this principle to inferences made by a computer, then *someone* (if not the officer, then perhaps a technical expert) must be able to articulate the facts and reasoning underlying the prediction—and

---

[306] *See supra* notes 212–19 and accompanying text.

[307] *See supra* notes 289–90 and accompanying text.

[308] *See supra* note 288 and accompanying text.

[309] *See supra* notes 239–44 and accompanying text. The wisdom of this articulability requirement has been questioned by law professor Richard E. Myers II, who argues that articulability is a "lawyer's standard," a legal fiction, and that "much of what matters to people in the world is incredibly difficult to reduce to language." Richard E. Myers II, *Challenges to* Terry *for the Twenty-First Century*, 81 MISS. L. J. 937, 938–47 (2012) ("[M]any . . . police officers[] may lack the linguistic capacity to successfully recount their experiences in language that lawyers and judges can use in court.").

justifying the officer's reliance on it—in a way that judges who are not technical experts can understand. Even if such testimony is feasible, there is likely to be some discrepancy between what the computer "knows" and what the officer knows at the time of the seizure. This discrepancy could bear on the officer's ability to judge whether the particular circumstances warranted a seizure.

Courts will likely consider the officer's training and experience with the prediction software. In the drug courier profile cases, courts were more likely to defer to officers' inferences drawn from the drug courier profile when the officers were knowledgeable about and experienced with applying the profile.[310] Courts may foreseeably emphasize the officer's knowledge about the reliability of the predictive software. For example, if an officer receives a prediction that an individual has an 80 percent likelihood of committing a crime, and the officer has knowledge or reason to believe that the predictive software has a very high reliability and accuracy level, courts may be more likely to defer to that officer's decision to stop the individual than if the officer had no knowledge of the software's reliability. Similarly, courts may be more likely to defer to officers who have had extensive experience using the software and who testify that, nine times out of ten, when they make stops based on the software's predictions, they find evidence of illegal activity. However, establishing sound metrics of automated predictive software's reliability and accuracy could take years of pilot testing and record keeping. In the mean time, since pilot testing involves the rights of real people, police action based on automated predictions is likely to come before a court.[311]

[310] *See supra* notes 212–19 and accompanying text.

[311] *See* Ferguson (2012), *supra* note 120, at 312.

Courts will have to grapple with how automated inferences, based on ones and zeros, will fit into what has heretofore been a highly context-dependent inquiry.

Automation, Officer Discretion, and Preventing Arbitrary Seizures

Courts may see the formulaic and automated nature of predictive software as a strength or a weakness—or possibly both. In his *Sokolow* dissent, Justice Marshall warned that a "law enforcement officer's mechanistic application of a formula of personal and behavioral traits in deciding whom to detain can only dull the officer's ability and determination to make sensitive and fact-specific inferences[.]"[312] Courts upholding profile-based stops have emphasized the ways in which officers avoided "mechanically matching" the suspect with a profile and instead relied on their "training and experience" to decide whether the observed facts "appeared suspicious."[313] An automated profile is necessarily even more "mechanistic" than an analog one. A computer makes predictions based on the same algorithm—the same pre-determined set of risk factors—applied to every potential suspect. These factors can change over time, but only in response to new data processed and new information learned by the computer—not in response to what the officer observes or learns. Officers will presumably have to exercise discretion by deciding how heavily to weigh and ultimately whether to act on the prediction, based on the system's reliability, the other circumstances at issue, and the officer's experience. Still, any decision that takes the automated prediction into account relies at least in part on a mechanistic application of a pre-determined profile.

---

[312] *Sokolow*, 490 U.S. at 13 (Marshall, J., dissenting).

[313] United States v. Colyer, 878 F.2d 469, 479 (D.C. Cir. 1989).

Critics of the drug courier profile—often the same ones who warn of overly mechanistic application—condemn its "chameleon-like" "malleability."[314] Courts have complained of the variable and even contradictory nature of the profile's factors from case to case.[315] Critics argue that officers' ability to tweak the profile factors to fit a given situation gives them too much leeway to create an after-the-fact justification for searches that were otherwise based on "mere hunches."[316] An automated profile would appear to solve this problem by disallowing officers from tweaking the risk factors to fit a given situation. The Second Circuit's treatment of the 1970s-era "highjacker profile" suggests that courts might give more deference to "objectively employed" profiles compiled based on "scientific, sociological[,] and psychological data[.]"[317] However, this deference to "objective" markers of suspicion applied "without [] any subjective interpolation"[318] is anomalous in Fourth Amendment reasonable suspicion law. Jurisprudence in this area almost always prizes officers' reasonable inferences above all else.[319] Thus, giving weight to the purported objectivity of automated predictions would significantly change the nature of the Fourth Amendment reasonable suspicion inquiry.

---

[314] *See Sokolow*, 490 U.S. at 13 (Marshall, J., dissenting); United States v. Wilson, 953 F.2d 116, 124 (4th Cir. 1991); United States v. Respress, 9 F.3d 483, 490 (6th Cir. 1993); United States v. Rodriguez, 976 F.2d 592, 595 (9th Cir. 1992); United States v. Jennings, 985 F.2d 562 (6[t]h Cir. 1993); LaFave, *supra* note 36, at 482.

[315] *See Respress*, 9 F.3d at 490.

[316] *See* Cloud, *supra* note 37, at 858; LaFave, *supra* note 36, at 482.

[317] *See* United States v. Bell, 464 F.2d 667, 669–70 (2d Cir. 1972).

[318] *Id.*

[319] *See, e.g.*, Ornelas v. United States, 517 U.S. 690, 696–97 (1996); *see generally* Colin D. Wood, *They Didn't Look Right to Me!: Reasonable Suspicion in Kansas: Through Whose Eyes Is It Viewed?*, 76 J. KAN. B.A. 16 (2007). This emphasis on officers' subjective inferences is often criticized, *see, e.g.*, Dana Raigrodski, *Reasonableness and Objectivity: A Feminist Discourse of the Fourth Amendment*, 17 TEX. J. WOMEN & L. 153, 172–82 (2008); Andrew Guthrie Ferguson & Damien Bernache, *The "High-Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment Reasonable Suspicion Analysis*, 57 AM. U. L. REV. 1587, 1607–15 (2008), but it remains the prevailing standard.

Both of these criticisms of drug courier profiles stem from courts' longstanding skepticism of uncabined officer discretion leading to arbitrary searches and seizures.[320] Courts must ask whether the use of automated predictions upholds the purpose of the Fourth Amendment to guard against arbitrary law enforcement action.[321] Some proponents of predictive policing would argue that automated predictions represent hard statistical probabilities, which can eliminate arbitrariness from and increase the objectivity of officers' decisions.[322] But courts would abdicate their responsibilities if they simply accepted this reasoning, or required only a showing that a predictive system and its underlying data were statistically reliable.

In the reasonable suspicion context, the Fourth Amendment protects against arbitrary seizures by requiring officers to testify to the "totality of the circumstances," including observed or previously known facts sufficient to give rise to suspicion.[323] Predictive algorithms are incapable of knowing or observing the "totality of the circumstances." They can only make inferences based on the statistical relationships they find in the data they have. The probativeness of these relationships may vary from one instance to another based on the totality of the circumstances. In one person, multiple risk factors associated with crime may be correlated with one another for innocent reasons—as was the case in *United States v. Ornelas Ledesma*, where the court found that Hispanic Americans were more likely to fit an iteration of the drug courier profile based on their

[320] *See* Terry v. Ohio, 392 U.S. 1, 12–13 (1968); INS v. Delgado, 466 U.S. 210, 215 (1984).

[321] *See Terry*, 392 U.S. at 12–13; *Delgado*, 466 U.S. at 215.

[322] *See, e.g.*, 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/#442d97b26931; Berg, *supra* note 7.

[323] *See* United States v. Sokolow, 490 U.S. 1, 7–8 (1989).

likelihood of being poor and transient rather than their likelihood of being criminals.[324] In another person, the same risk factors may be independent and highly probative of criminal activity. Officers are ultimately and unavoidably responsible for determining how much weight to give to an automated prediction in light of the surrounding circumstances. Thus, the Fourth Amendment requires courts to evaluate the interplay between the prediction—including its underlying analysis—and the officer's knowledge and judgment.

Ultimately, the reasonableness of a profile depends not on its rigidness or malleability but on its ability to sufficiently narrow the specter of suspicion. Profiles are unconstitutionally broad if they would subject "significant numbers of innocent persons" to "virtually random seizures."[325] Officers, and ultimately courts, must determine whether automated profiles sufficiently limit the number of potential suspects who fit them. This is where the statistical nature of automated profiles may help by making it feasible to determine the percentage of the population that fits a particular profile.[326] The task of determining narrowness may be better facilitated by some systems than by others. For example, a system that predicts a person's likelihood of committing a crime as a percentage may help officers eliminate large numbers of innocent persons from suspicion. Officers could adopt a policy of requiring a very high likelihood (say 80% or higher) before taking the prediction seriously. On the other hand, systems such as Beware that attempt to categorize all individuals into three broad risk categories (red, yellow, and

[324] United States v. Ornelas-Ledesma, 16 F.3d 714, 716–17 (7th Cir. 1994).

[325] Reid v. Georgia, 448 U.S. 438, 441 (1980).

[326] In *United States v. Colyer*, the D.C. Circuit held that a profile used to stop an Amtrak customer was sufficiently narrow when an Amtrak agent testified that investigations based on the profile "would typically reveal no more than three suspicious reservations on a 400-seat train." United States v. Colyer, 878 F.2d 469, 482 (D.C. Cir. 1989).

green) may be less easily parsed and more susceptible to sweeping in large numbers of people.

Consensual Encounters and "Surveillance Discretion"

Although this analysis has focused on Fourth Amendment seizures, automated profiling is perhaps more likely to lead to law enforcement interventions that do not fall under the Fourth Amendment's protections.[327] Chicago's Custom Notifications program, for example, directs officers to visit at-risk individuals' homes and inform them of the consequences of committing violent crimes.[328] Such "knock-and-talks" are considered consensual encounters and do not fall under the Fourth Amendment's reasonable suspicion or probable cause requirements.[329] Police need not have any particular level of suspicion or justification for simply approaching an individual—at her residence or in public—and asking questions. Thus, law enforcement can use automated profiling as a "starting point" for investigations without triggering Fourth Amendment protections. Law Professor Elizabeth Joh has referred to law enforcement decisions "to focus police attention on a particular person" as "surveillance discretion."[330] There are few if any legal limits on surveillance discretion.[331] However, arrests often develop from consensual encounters when questioning yields information that gives police probable cause.[332] In

[327] *See* INS v. Delgado, 466 U.S. 210, 215 (1984) (delineating Fourth Amendment seizures from police conduct that falls short of a seizure and does not fall under Fourth Amendment protection).

[328] *See supra* notes 1–6 and accompanying text.

[329] *See* Florida v. Jardines, 133 S. Ct. 1409, 1415–16 (2013).

[330] Joh, *Surveillance Discretion*, *supra* note 121, at 15, 17.

[331] *See id.*

[332] *See Delgado*, 466 U.S. at 215 (citing United States v. Mendenhall, 446 U.S. 544, 554 (1980) ("[A]n initially consensual encounter between a police officer and a citizen can be transformed into a seizure or

these situations, courts should pay close attention to the extent to which automated predictions factored into the decision to approach and ultimately arrest an individual.

Automated predictive software is designed to aid in the early prevention of crime, lending itself more to non-Fourth Amendment interventions than to *Terry* stops, which require temporal exigency.[333] Algorithms predict what is likely to happen at some point in the future, but they do not necessarily indicate that someone is in the middle of committing, has committed, or is about to commit a crime. Thus, automated predictions can more aptly assist with law enforcement efforts to seek out an individual and conduct a "consensual" intervention rather than with *Terry* stops, which are associated with chance encounters—when police officers happen to observe individuals acting suspiciously. The potential social and policy implications of these prediction-based "consensual" encounters will be discussed in Chapter Four.

Conclusion

This chapter has drawn seven important inferences about how courts might apply Fourth Amendment law to automated profiling predictions. First, the Fourth Amendment requires courts to judge reasonable suspicion based on the individualized facts in each case, and this standard likely precludes courts from giving "blanket" or binding approval to the use of automated predictions to justify seizures. Second, officers relying on automated predictions will have to make some showing as to the specific factors and rationales underlying the automated prediction, but the information may be allowed to remain under seal. Third, incorporating automated predictions into the reasonable

detention within the meaning of the Fourth Amendment, 'if, in view of all the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave.'").

[333] *See supra* notes 1–6 and accompanying text.

suspicion calculus will necessarily shift the focus of the inquiry away from the officer's experience, knowledge, observations, and inferences. Courts must grapple with discrepancies between the officer's knowledge and the computer's "knowledge." Fourth, officers' knowledge of and experience with the automated prediction software at issue will likely be an important factor in the determination of whether the officer acted reasonably. Fifth, courts must ensure that the deployment of automated predictions does not lead to arbitrary seizures by, for example, giving undue weight to certain characteristics that may not be particularly probative of crime. Sixth, courts must also ensure that automated prediction software is used in a way that allows officers to use their discretion to judge the reliability and appropriateness of predictions in light of the totality of the circumstances. Finally, it is possible for automated profiling to avoid Fourth Amendment scrutiny altogether by operating in the background to guide "surveillance discretion." The next chapter will discuss some of the potential social and policy implications of automated profiling.

CHAPTER 4: POLICY CONSIDERATIONS FOR AUTOMATED PROFILING

Introduction

So far, this thesis has analyzed how Fourth Amendment reasonable suspicion law might apply to automated profiling. However, the legality of automated profiling should not be the only question police departments and governments consider before implementing this technology into policing practices. Automated predictive models come with a particular set of limitations and risks that should be acknowledged in any policy decisions to implement and regulate the use of such models. The purpose of this chapter is to discuss these considerations.

This chapter proceeds in seven sections. The first four sections discuss specific aspects of automated predictive software and its implementation that should be addressed by the data scientists who design predictive software, the law enforcement agencies that implement it, and the policymakers that regulate it. Section A discusses the relevance of the underlying factors that automated prediction software might consider when making predictions. Section B discusses reliability issues that can arise when computers use big data to predict crime. Section C discusses the ways in which bias can enter the automated decision-making process and lead to disparate treatment of minority groups. Section D discusses the importance and the challenge of maintaining government transparency when using automated predictive policing software.

The final three sections address broader concerns about the philosophy and objectives underlying the adoption of automated profiling tools. Section E discusses the modern trend of numbers-based policing and its capacity to skew police priorities away from protecting the holistic well-being of communities. Section F discusses the phenomenon of system avoidance and the ways in which automated profiling might exacerbate system avoidance. Finally, Section G contemplates a right to be unpredictable, a liberty interest based on the social value of autonomy that may be threatened by overreliance on predictive policing.

Relevance[334]

Predictive analytics identify connections and patterns, in a process called "link analysis," and apply those patterns to predict future outcomes.[335] But not all statistical links are relevant, if relevance is defined as being meaningfully probative of future criminal activity. This section discusses three aspects of automated predictive policing software that might obscure the relevance or irrelevance of statistical links: (1) the deliberate search for non-obvious relationships; (2) "signal-to-noise" issues that confuse the relative strength of relationship; and (3) the potential lack of a clear logical nexus between variables.

Some automated systems are designed to find subtle, "non-obvious" connections, which can skew analysis toward over-prediction at the expense of true relevance.[336] Non-Obvious Relationship Analysis ("NORA") tools "can identify links and relationships not readily identifiable using traditional link analysis software."[337] NORA's application to

---

[334] The term "relevance" as used in this thesis refers to facts that are meaningfully probative of future criminal activity. This requires not only a statistical link but also some logical nexus.

[335] *See* COLLEEN MCCUE, DATA MINING AND PREDICTIVE ANALYSIS: INTELLIGENCE GATHERING AND CRIME ANALYSIS 15 (2006).

[336] *Id.* at 45.
[337] *Id.*

law enforcement is based in part on the premise that sophisticated or organized criminals may intentionally obscure their information and associations.[338] These analytical tools are more sensitive to subtleties.[339] However, there is a direct tradeoff between this sensitivity and ensuring that the links identified are relevant.[340] Data scientist Colleen McCue's primer on predictive analytics provides an example of this tradeoff: "[NORA] tools [] can identify subtle changes in numeric information, such as social security numbers. In many cases, these transpositions are unintentional keystroke errors. In others, however, numeric information is changed slightly to reduce the likelihood that information will be linked directly, which can be indicative of identity theft or similar types of fraud."[341] Thus, there is a chance that a slightly altered social security number is indicative of identity theft, but it is more likely that the transposition means nothing. In this example, the subtlety of the link is inversely correlated with its probative value. While this sensitivity can be beneficial in some contexts, predictions that inform police interventions should err on the side of accuracy, since basic freedoms may be at stake and errors can be costly.

Link analysis can show not only the existence of relationships but also their relative strength.[342] If not carefully calibrated, however, automated systems can overstate the link strength, making connections seem stronger than they are.[343] These errors are

---

[338] *Id.*

[339] *Id.*

[340] *See, e.g.*, *id.* at 18–20.

[341] *Id.* at 45.

[342] *Id.* at 15.
[343] *Id.* at 15–16.

caused by "uneven distributions" causing "signal-to-noise issues."[344] For example, algorithms may try to measure the strength of associations between individuals by analyzing the number of times those individuals have called one another.[345] Analysts can set thresholds such that twenty calls indicate a strong relationship.[346] However, some people make significantly more phone calls than others. People who make hundreds of calls per week may easily cross this twenty-call threshold with many of their contacts, while people who make fewer than twenty calls per week will appear to have no strong relationships. Thus, the relevance of phone calls may be underestimated or overestimated because of the thresholds and units of measurements chosen by analysts.[347]

Determining relevance requires an understanding of the logical nexus between two statistically connected factors. The drug courier profile, for example, is composed of factors whose relationships to criminal activity can be intuited. Traveling under an alias,[348] not checking baggage,[349] and appearing nervous[350] all are associated with fearing detection or trying to avoid detection; common sense dictates that a person selling narcotics would likely be traveling from a city known as a source of these drugs[351] and that a person involved in a drug transaction might be carrying an unusually large amount

---

[344] *Id.*

[345] *See id.* at 15–17.

[346] *See id.* at 15–16.

[347] *See id.* at 15–17.

[348] United States v. Elmore, 595 F.2d 1036, 1039 n.3 (5th Cir. 1979).

[349] *Id.*

[350] *Id.*

[351] *Id.*

of currency.[352] Each of these characteristics can describe innocent travelers, but each one bears a clear (if tenuous)[353] relationship to the crime (or at least *a* crime). However, since automated systems are meant to surpass common sense,[354] the links they discover might not share a readily discernible logical nexus. Some would argue that this is the point of automation—its added value is that it finds "surpris[ing]" patterns.[355] McCue explained this value in terms of Wal-Mart's success with predictive analytics:

> [W]hat can we learn from Wal-Mart and Amazon about fighting crime in a recession? . . . Wal-Mart as an organization has effectively leveraged large amounts of historical point-of-sale data in an effort to anticipate and effectively respond to their customers. In one particular example, the analysts at Wal-Mart noted unique patterns of purchasing behavior in advance of a major weather event. Specifically, sales of bottled water, duct tape, and Pop-Tarts increased in the period of time immediately preceding a storm. While the bottled water and duct tape are obvious choices . . . the increased sales of Pop-Tarts is surprising. Therefore . . . the bottled water and duct tape represent "confirmation," and the increased sales of Pop-Tarts would be "discovery" of new and ideally actionable relationships. It is important to note that while we can consider the possible motivations behind this behavior (e.g., Pop-Tarts are easy to store and prepare, do not require refrigeration, can be eaten directly out of the box), *understanding the underlying reason for this is not necessary for it to be actionable*. Knowing that consumers will be purchasing Pop-Tarts in anticipation of a major weather event is sufficient for Wal-Mart to adjust their supply chain and meet the need.[356]

---

[352] *Id.*

[353] *See* Cloud, *supra* note 37, at 846 ("Unfortunately, the validity of many of these profile characteristics is questionable because some fail to describe the actual behaviors of drug couriers and others are so vague they permit police officers to act upon impermissibly subjective hunches.").

[354] *See supra* notes 336–41 and accompanying text.

[355] MCCUE, *supra* note 335, at 35.

[356] *Id.* at 31–32 (emphasis added).

In this example, McCue is probably correct that Wal-Mart does not need to know *why* people are buying Pop-Tarts before a storm in order to decide that it should increase its Pop-Tart supply. However, if Wal-Mart is wrong about the Pop-Tart-storm connection—if sales are increasing for some reason unrelated to the storm—the only consequences are a surplus of Pop-Tarts and a very modest potential loss of profits. In the law enforcement context, faulty inferences can mean surveilling or even arresting the wrong person, or failing to stop a crime. The stakes are much higher, and the rigor of analysis should be higher as well.

Reliability[357]

Predictive models and the data they analyze must be reliable. This section discusses several factors that can compromise the reliability of automated profile-based predictions in the law enforcement context. First, inherent limitations in crime-related datasets can lead to flawed predictive models. Second, the reliability of predictive models can be difficult to evaluate because the models rely on changing the future by preventing crime and because they can create self-fulfilling prophecies by concentrating police attention on certain people.

[357] In general, reliability refers to the ability of the datasets and the results of the prediction models to reflect reality. In the context of crime data, this means that the data on instances of a certain crime are actually representative of the instances of those crimes in reality—where they occur, who commits them, etc. Data can be unreliable because it is inaccurately recorded, because not enough records exist to construct a complete and representation of reality, or because the records that exist overrepresent or underrepresent certain characteristics. Predictive models are reliable if their predictions tend to be accurate. Thus, automated profiling predictions are reliable if the individuals they predict as having a high likelihood of committing crimes are actually highly likely to commit crimes.

Data Reliability

Unreliable data can compromise automated predictions. In order to be reliable, the data that "teach" an algorithm how to predict a certain type of crime must accurately represent that crime. This is especially difficult to achieve in the law enforcement context for at least three reasons: (1) data about criminals is limited to those who got caught; (2) law enforcement recordkeeping practices have been historically inconsistent; and (3) more serious crimes, such as violent crimes, are relatively infrequent events. These factors tend to create data samples that are small, incomplete, and unrepresentative.

Even if one had access to all records related to crime, the individuals represented in these data would be limited to those who have had some contact with the criminal justice system; the known criminals would only represent those who had been "caught."[358] Because of the limits of collecting crime data, "almost everything that we know about crime and criminals is based on a relatively small [sample] of information gathered from only a fraction of all criminals[.]"[359] The sample is non-random, which makes it inherently less reliable than a random sample.[360] From this already limited universe of information, analysts must compile and "scrub"[361] data to create reliable samples from which automated systems can learn and develop rules for making predictions.

---

[358] *Id.* at 5–6.

[359] *Id.* at 6.

[360] *Id.* at 7.

[361] Data Scrubbing, TECHOPEDIA, https://www.techopedia.com/definition/14651/data-scrubbing.

The task of creating reliable samples is further complicated by law enforcement agencies' history of faulty recordkeeping practices.[362] For example, some jurisdictions do not require police officers to record investigative stops that do not result in arrests.[363] Thus, data on these types of stops do not adequately represent the number or nature of false positives. The incomplete nature of available crime data means that even carefully scrubbed samples may be too small and unrepresentative to create reliable outcomes.

Some predictive policing models use commercially collected digital data, which is even less reliable than government records. For example, Beware, a pilot program in Fresno, California, that assigns "threat scores" of green, yellow, or red to individuals, uses information from commercial data brokers.[364] Data brokers comb the Internet and compile available data on individuals. This can include everything from criminal records to social media activity to health information. Internet companies and data brokers are economically incentivized to collect as much information as they can, regardless of its accuracy. Information collected for one purpose is often compiled with other information and used for unanticipated purposes. The rules under which the data were originally collected may be unknown. For example, a commercial database may purport to show the names of individuals who have purchased assault weapons online, but it may not disclose how it defined "assault weapon." Without knowing the collection rules and the reliability

[362] *See, e.g.*, David Curry, Richard A. Ball, & Robert J. Fox, *Gang Crime and Law Enforcement Recordkeeping*, NIJ RESEARCH IN BRIEF (1994), https://www.ncjrs.gov/txtfiles/gcrime.txt (explaining that national data on gang violence was difficult to obtain because jurisdictions varied in recording practices).
[363] *See* ACLU OF ILLINOIS, STOP AND FRISK IN CHICAGO (March 2015), http://www.aclu-il.org/wp-content/uploads/2015/03/ACLU_StopandFrisk_6.pdf.

[364] *See* Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score'*, WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html; David Robinson, *Buyer Beware: A Hard Look at Police 'Threat Scores'*, EQUALFUTURE (Jan. 14, 2016), https://www.equalfuture.us/2016/01/14/buyer-beware-police-threat-scores/.

controls employed by the original collecting entity, analysts may be less able to verify the reliability of these datasets.[365]

The types of crimes that automated systems might attempt to predict, such as sexual assaults, murders, and other violent crimes, are "infrequent events," which are inherently difficult to statistically predict.[366] Predicting a specific type of crime requires exposing the predictive model to information about past crimes of the same type. The model learns the characteristics and factors associated with that crime and—in the case of automated profiling—with the individuals who commit those crimes. For relatively rare events, such as murders, the event sample size is small. The smaller the sample size, the more susceptible it is to statistical error, and the less reliable the results and predictions will be.[367] As data scientist and predictive analytics expert Colleen McCue put it, "the fact that [violent crime] is a relatively infrequent event is a very good thing for almost everyone, except the analysts."[368]

McCue's research shows that data on infrequent events can create flawed predictive models. She set out to create a model that would predict whether an armed robbery would escalate into an aggravated assault. However, the data showed that armed robberies escalated into aggravated assaults less than five percent of the time, making "robbery-related aggravated assaults" an infrequent event. McCue found that

> a very simple model can be created that has an accuracy rate of greater than 95%. In other words, this simple model could correctly predict the escalation of an armed robbery into an aggravated assault 95% of the time. At first blush,

[365] *See* MCCUE, *supra* note 335, at 14–15.

[366] *Id.* at 8–10.

[367] *Id.*

[368] *Id.* at 8.

> this sounds phenomenal. . . . Examining the model further, however, we find a critical flaw: There is only one decision rule, and it is "no." By predicting that an armed robbery will never escalate into an aggravated assault, the model would be correct 95% of the time, but it would not be very useful.[369]

This example illustrates the importance of carefully parsing and evaluating the rules that automated systems use to make predictions.

Falsifiability[370]

The reliability of predictive models must be continually evaluated in the real world. Gathering and evaluating information about these systems' accuracy rates may be complicated by at least two factors. First, when interventions are designed to prevent individuals from committing future crimes, it may be difficult to distinguish between successful interventions and false predictions. Imagine a police officer in Chicago receives a prediction that a resident is likely to commit a violent crime. The officer visits the resident's home as part of Chicago's Custom Notifications program[371] and warns the resident about the consequences of committing violent crimes. If the resident is never caught committing, arrested for, or charged with a crime, how do police know whether the resident was deterred or if she never would have committed a crime in the first place? Should this be categorized as a successful intervention or a false prediction? Automated models whose success is based on changing the future might evade meaningful tests of reliability.

[369] *Id.*

[370] Falsifiability refers to the ability of the models' accuracy to be tested.

[371] *See supra* notes 1–6 and accompanying text.

Second, automated predictions used to inform surveillance discretion can create "feedback loops" or "self-fulfilling prophecies" that inflate accuracy levels.[372] One of the likeliest uses of automated predictions will be to help police make decisions about whom to further surveil and investigate.[373] Police are more likely to observe crime wherever they are focusing their surveillance.[374] Thus, if predictions are used to train surveillance on specific individuals, those individuals are more likely to be caught committing crimes than are individuals who aren't being closely watched. As predictive models learn from these results, over-reliance on predictions threatens to create a feedback loop in which predictions become increasingly focused on individuals with similar characteristics. In addition to disproportionately targeting minority groups, these results can obscure potential weaknesses in the models' accuracy.

Bias and Discrimination

Big data analytics are not inherently neutral. As Solon Barocas and Andrew Selbst have noted, "[T]he very point of data mining is to provide a rational basis upon which to distinguish between individuals."[375] Therefore, "[b]y definition, data mining is *always* a form of statistical (and therefore seemingly rational) discrimination."[376] Data mining and predictive analytics have been described as "brutally objective."[377] Indeed, predictive automated profiling systems make distinctions between or categorize

[372] *See* Steven J. Ellwanger, Predictive Policing 698, *in* ENCYCLOPEDIA OF CRIMINAL JUSTICE ETHICS (Bruce A. Arrigo, ed. 2014).

[373] *See supra* notes 327–33 and accompanying text.

[374] *See generally* HARVEY A. SILVERGLATE, THREE FELONIES A DAY: HOW THE FEDS TARGET THE INNOCENT (2009).

[375] Barocas & Selbst, *supra* note 28, at 7.

[376] *Id.*

[377] McCue, *supra* note 335, at 38.

individuals based on statistical relationships objectively found in the input data. But the objective, unbiased nature of this process, and its ability to be an antidote for human bias and invidious discrimination, are often overstated. There are multiple opportunities throughout the data collection and coding processes for bias to skew the results of data mining. First, the datasets used to "teach" or train an algorithm can reflect individual and social biases that can be encoded into predictive models. Second, designing algorithms requires some human intervention. Humans can intentionally or unintentionally design algorithms that parse information in ways that disadvantage certain groups. At best, undetected and uncorrected bias can lead to unreliable predictions. At worst, it can result in predictive systems that discriminate against minority groups.

Data Bias

Automated predictions are only as good as their "training data"—the data from which algorithms learn relationships and patterns that they can use to make distinctions.[378] Barocas and Selbst have catalogued several ways in which biased training data can skew results and lead to unfair discrimination.[379] This section applies their research to the predictive policing context.

Existing data can reflect human subjectivity and societal biases. According to Barocas and Selbst, "[I]f data mining treats cases in which prejudice has played some role as valid examples from which to learn a decision-making rule, that rule may simply reproduce the prejudice involved in these earlier cases."[380] This concern is particularly salient in the law enforcement context. Countless studies, investigations, and commentary

---

[378] Barocas & Selbst, *supra* note 28, at 10.

[379] *Id.* at 10–11.

[380] *Id.*

are dedicated to the role that bias—particularly racial bias—plays in police officers' decisions to stop, search, and arrest individuals.[381] These biases can also factor into convictions, sentencing, and parole decisions.[382] Moreover, the role of bias in these decisions is difficult to detect. If it goes unchallenged, bias is unlikely to be detected. Thus, it is plausible that automated prediction software will treat a high number of cases in which bias played a role as legitimate. The racial or other biases of individual police officers and of society at large can be encoded into predictive algorithms.

Relatedly, data samples can over- or under-represent certain minority groups. According to Barocas and Selbst, "[I]f data mining draws inferences from a biased data sample of the population to which inferences are expected to generalize, any decision that rests on these inferences may systematically disadvantage those who are under- or over-represented in the dataset."[383] It is well documented that black men and women make up a disproportionately large percentage of those stopped by police, arrested, and imprisoned. Forty percent of people incarcerated in the United States are black, despite the fact that only 13 percent of the U.S. population is black.[384] Although studies show that people of color are no more likely to sell illegal drugs than whites, they have faced higher rates of drug arrests.[385] Blacks and Hispanics are also more likely to be searched

---

[381] *See, e.g.*, Joshua Correll, et al., *Across the Thin Blue Line: Police Officers and Racial Bias in the Decision to Shoot*, 92 J. PERSONALITY & SOC. PSYCH. 1006 (2007).

[382] *See, e.g.*, Gary Kleck, *Racial Discrimination in Criminal Sentencing: A Critical Evaluation of the Evidence with Additional Evidence on the Death Penalty*, 46 AM. SOC. REV. 783 (1981).

[383] Barocas & Selbst, *supra* note 28, at 10–11.

[384] United States Profile, Prison Policy Initiative, http://www.prisonpolicy.org/profiles/US.html#disparities (last visited Dec. 11, 2015).

[385] *US: Drug Arrests Skewed by Race*, HUMAN RIGHTS WATCH (Mar. 2, 2009), https://www.hrw.org/news/2009/03/02/us-drug-arrests-skewed-race.

during a traffic stop than whites.[386] Since predictive policing relies on existing data to identify patterns, overrepresentations of racial minorities in the data could lead to discriminatory algorithms that reflect historical and persisting societal bias.

For a real-world example of how biased data can skew results and disadvantage minorities, consider the smart phone application Street Bump. Street Bump detects and reports potholes in Boston by collecting data from residents' smart phones as they drive through the city.[387] In her article, *Think Again: Big Data*, Kate Crawford warned that "whatever information the city receives from [Street Bump] will be biased by the uneven distribution of smartphones across populations in different parts of the city."[388] This could result in underreporting and under-repairing of road problems in low-income communities where fewer people have smartphones. It is not enough for training datasets to be accurate and complete. Datasets should not be used to train predictive models unless analysts can come up with ways to find and correct for implicit bias.

<u>Coding Bias</u>

The word "automated" tends to evoke a process free of human intervention, but even automated, machine-learning systems involve some human subjectivity. The target variable that an algorithm is designed to determine (e.g., creditworthiness, likelihood of committing a crime) must be operationalized as variables that algorithms can discern

---

[386] U.S. DEP'T OF JUSTICE, POLICE BEHAVIOR DURING TRAFFIC AND STREET STOPS, 2011 (Sept. 2013), http://www.bjs.gov/content/pub/pdf/pbtss11.pdf.

[387] STREET BUMP, http://www.cityofboston.gov/DoIT/apps/streetbump.asp (last visited December 3, 2015); *see* Kate Crawford, *Think Again: Big Data*, FOREIGN POL'Y (May 10, 2013), http://foreignpolicy.com/2013/05/10/think-again-big-data/.

[388] Crawford, *supra* note 387.

(e.g., good credit history, low education level).[389] "Through this process of translation, [] data miners may unintentionally parse the problem and define the target variable in such a way that protected classes happen to be subject to systematically less favorable determinations."[390] The more complex and nuanced the target variable, the more human subjectivity will play into defining it. The likelihood that someone will commit a crime is shaped by an infinite number of factors, many of which are likely unobservable or unquantifiable (e.g., subjective state of mind). One Chicago program focuses on social connections within and between gangs, mapping people's associations to attempt to determine who might commit a murder in the near future.[391] Thus, this program has defined "likelihood of committing murder" as "connectivity to certain gang members." This may be a rational way of distinguishing between people who are likely and unlikely to commit murders. But it may also subject certain classes of people—likely young black males—to disproportionate scrutiny.

Even when predictive algorithm programmers are careful not to use race or class as factors, proxies for race and class may be introduced into the algorithm.[392] As Barocas and Selbst have explained, this happens when "criteria that are genuinely relevant in making rational and well-informed decisions also happen to serve as reliable proxies for class membership."[393] These proxies tend to reveal existing historical inequalities. For

---

389 Barocas & Selbst, *supra* note 28, at 7–8.

390 *Id.* at 8. Danielle Keats Citron describes the same problem in a different way. In the federal agency context, she writes that "[c]omputer programmers inevitably engage in rulemaking" when they translate agency rules into code (which ultimately determines outcomes). Citron, *supra* note 90. However, this type of rulemaking happens without the notice and review required of traditional rulemaking. *Id.*

391 Dokoupil, *supra* note 1.

392 Barocas & Selbst, *supra* note 28, at 20–21.

393 *Id.* at 21.

example, in the employment context, members of historically marginalized classes are more likely to lack the markers traditionally associated with prospective job success, such as education from an elite institution.[394]

It is not difficult to imagine factors that may be associated with crime but are also proxies for race and class. As noted earlier, Chicago's targeting of gang members likely affects predominantly young black men. Questionnaires designed to evaluate the likelihood of recidivism in parole candidates have asked about demographic factors such as education level and employment status,[395] factors that also inversely correlate with being black and poor.[396]

Discrimination by proxy may be particularly difficult to detect in an algorithm that uses computer learning to develop patterns. As algorithms learn, they begin to *decide* which factors are relevant to the target variable.[397] Thus, police officers using the algorithm—and even the analysts who created it—may lack knowledge or control over the factors the algorithm is using and the weight it is assigning to those factors. This can make subtler forms of discrimination difficult to detect.[398] The next section will address the opacity of algorithms more broadly.

---

394 *See id.*

395 *The New Science of Sentencing*, THE MARSHALL PROJECT (Aug. 4, 2015), https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing; Barry-Jester, et al., *supra* note 8.

396 KATHLEEN SHORT, U.S. CENSUS BUREAU, THE SUPPLEMENTAL POVERTY MEASURE 5–6 (2014) (Table 2).

397 *See* Citron & Pasquale, *supra* note 93, at 5–6 (describing how artificial intelligence eventually cuts out the human middle man).

398 *See, e.g.*, Barocas & Selbst, *supra* note 28, at 2.

Transparency

The accountability of and the public's trust in law enforcement agencies depend upon adequate transparency. The requirement that police officers be able to justify stops, searches, and seizures serves not only to protect people from arbitrary police action but also to provide an opportunity to challenge actions perceived as unjust infringements on liberty and privacy.[399] This premium on transparency does not change when officer discretion is replaced by an algorithm that decides who should be a potential suspect. Yet police departments have been unwilling to release the predictive policing algorithms they use, or any details about how the algorithms work and what factors they look for.[400] In their article, *The Scored Society*, Danielle Citron and Frank Pasquale warned that predictive algorithms are "zealously guarded" and "shrouded in secrecy," and therefore their decisions cannot be effectively challenged.[401]

Transparency and accountability in policing are enforced in part by courts, which require officers to justify challenged searches and seizures.[402] When automated prediction-based seizures are challenged in court, if officers are not required to testify to the factors underlying the predictions, or if they are allowed to shield such testimony

---

[399] *See* Terry v. Ohio, 392 U.S. 1, 13–14 (1968).

[400] *See* BIG DATA FAIRNESS REPORT, *supra* note 1.

[401] Citron & Pasquale, *supra* note 93, at 5. In the government agency context, Citron argued that this raises due process issues, since rulemaking and adjudications are performed automatically without the requisite notice and opportunity for review. Citron, *supra* note 90, at 1254.

[402] *See supra* Ch. 2.B.

from public disclosure,[403] the public will lose out on this detailed record of what police officers consider when they decide whether they have reasonable suspicion or probable cause to make a stop, search, or arrest. If police officers are going to seize individuals based on an automated profile, that profile effectively becomes a rule or policy that determines outcomes.[404] As with other agency rules, the public is entitled to notice.[405]

Aside from institutional secrecy, a special barrier to transparency of automated predictive policing may be the nature of the automation itself. Algorithms may be opaque to the police officers who use them.[406] As algorithms learn new information, they continually adapt their decision-making formulae, which makes it easy for programmers or police officers to lose sight of precisely how decisions are being made. This can make discrimination and bias difficult to detect.[407]

The limitations addressed so far concern specific aspects of automated prediction software and its implementation that raise policy challenges. These issues presumably can be addressed in the design, evaluation, and implementation of automated profiling systems. The following sections of this chapter address broader concerns about the philosophy and objectives underlying the adoption of automated prediction tools that attempt to quantify suspicion and sort individuals into risk categories.

---

[403] *See* United States v. Bell, 464 F.2d 667, 669–72 (2d Cir. 1972) (requiring agents to testify to the factors comprising a confidential "hijacker profile" but allowing them to bar the public and defendant (but not the defendant's counsel) based upon "the compelling urgency of protecting the confidentiality of the profile which has been devised as a method to reduce the threat of hijacking").

[404] *See* Cloud, *supra* note 37, at 857 (characterizing the drug courier profile as "a formula allegedly answering [F]ourth [A]mendment questions" and as a "litmus-paper test"); LaFave, *supra* note 36, at 481 (characterizing the profile as a law enforcement "guideline" that would help determine questions of Fourth Amendment law); *see generally* Citron, *supra* note 90, (referring to programming predictive algorithms as a form of agency rulemaking).

[405] *Se generally* Citron, *supra* note 90.

[406] *See* Barocas & Selbst, *supra* note 28, at 1.

[407] *Id.*

Policing by the Numbers

Predictive policing epitomizes a modern law enforcement culture that prioritizes statistics and measures success in terms of crime reduction. Predictive policing can be seen as an extension of the CompStat era of law enforcement. CompStat is a set of data-driven policing methods introduced in the 1990s and used by police departments throughout the nation.[408] It refers to a range of programs and methods through which police attempt to understand, control, and prevent crime using data analytics.[409] CompStat's introduction was accompanied by required quotas for patrol officers and by "broken windows policing," both of which were aimed at reducing overall crime rates by targeting small crimes, such as panhandling and loitering.[410] While CompStat has been widely heralded for dramatically reducing crime in New York City,[411] it has also been criticized for shifting the focus of policing to an over-emphasis on crime control at the expense of protecting democratic values.[412] Starting in the 1990s, policing success came to be measured exclusively by crime rates. This mentality is associated with aggressive policing programs, such as stop-and-frisk, which have harmed police-community relations.[413]

---

[408] *See* DAVID WEISBURD, ET AL., POLICE FOUNDATION REPORTS, THE GROWTH OF COMPSTAT IN AMERICAN POLICING (2004), http://assets.lapdonline.org/assets/pdf/growthofcompstat.pdf.

[409] *Id.*

[410] *See generally, e.g.*, Nathaniel Bronstein, *Police Management and Quotas: Governance in the CompStat Era*, 48 COLUM. J.L. & SOC. PROBS. 543 (2015).

[411] *See* Weisburd, *supra* note 408.

[412] *See generally* Peter Hanink, *Don't Trust the Police: Stop Question and Frisk, CompStat, and the High Cost of Statistical Over-Reliance in the NYPD*, J. INST. JUSTICE & INT'L STUDIES 99 (2013).

[413] *Id.* at 100.

Law enforcement rhetoric around predictive policing takes this crime-control mentality to the next level. According to McCue, "[O]nce we can anticipate or predict crime, we will have the ability to prevent it."[414] This statement is not only problematic because it assumes the success of predictive policing and the omnipotence of data. It also minimizes the notion that police should focus on understanding and ameliorating the broader social forces that contribute to crime. As Elizabeth Joh has argued,

> [A] technocratic solution to crime is not the only objective of democratic policing. Reducing crime is not the only job of the police. Policing as an institution has never been amenable to a single objective, and indeed over time its aims have shifted. What is clear, however, is that democratic policing aims at more than mere crime control and, at its core, relies on skills that do not always lend themselves to statistical analysis. No amount of data-driven policing is likely to assuage communities scoured by long histories of tension with the police. Nor will demonstrations of little red boxes on a smartphone necessarily justify to a community the need for a heavy-handed police presence.[415]

Undue reliance on automated predictions can dull officers' perceptions. As McCue has pointed out, a predictive mindset does not always benefit police investigations.[416] "[E]stablishing a mindset early in an investigation can significantly affect interpretation of subsequent leads and clues, allowing important evidence to be overlooked . . . ."[417] There is no amount of data or magical formula that will lead to perfect or even near-perfect crime control; prioritizing data at the expense of holistic community policing is a fool's errand.

---

[414] MCCUE, *supra* note 335, at 34.
[415] Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 66–67 (2014).

[416] MCCUE, *supra* note 335, at 13.

[417] *Id.*

System Avoidance

As this thesis has suggested, predictive automated profiling systems are likely to lead to more non-Fourth Amendment, or "consensual" encounters.[418] Courts maintain that these non-seizure police contacts work such small or negligible encroachments upon liberty and privacy interests that they do not trigger constitutional protections.[419] But a recent study suggests that even low-level contact with police and the criminal justice system can have negative consequences. In an empirical study, Sarah Brayne found that individuals who have had contact with police are significantly "less likely to interact with surveilling institutions, [such as] medical, financial, labor market, and educational institutions, than their counterparts who have not had criminal justice contact."[420] Brayne has labeled this phenomenon "system avoidance," and she found it even in individuals who had low-level contact with the system.[421] Brayne noted that the effects of system avoidance may exacerbate marginalization along racial and class lines:

> Because criminal justice contact is disproportionately distributed . . . system avoidance is a potential mechanism through which the criminal justice system contributes to social stratification: it severs an already marginalized subpopulation from institutions that are pivotal to desistance from crime and their own integration into broader society.[422]

[418] *See supra* Ch. 3.

[419] *See supra* Ch. 2.

[420] Sarah Brayne, *Surveillance and System Avoidance: Criminal Justice Contact and Insitutional Attachment*, 79 Am. Soc. Rev. 367, 367 (2014). "By contrast, individuals with criminal justice contct are no less likely to participate in civic or religious institutions." *Id.*

[421] *Id.*

[422] *Id.*

By increasing the frequency of police contact with civilians, predictive policing may encourage avoidance not only of traditional institutions but also of online activities. Evidence suggests that predictive policing models are designed to incorporate data about online activity, such as social networking.[423] Websites, social media platforms, email providers, and cellular service providers are known for their record keeping. Individuals who want to avoid creating a digital trail because they are wary of surveillance may avoid using these tools. Today, email, social media, and online commerce are just as important as —if not more important than—traditional institutions for "integration into broader society."[424] This could widen the existing socioeconomic digital divide[425] and inhibit people from filling out online job applications, communicating with others, and pursuing knowledge and entertainment.

Brayne's research corroborates anecdotal accounts of system avoidance. In her ethnography, *On the Run: Fugitive Life in an American City*, Alice Goffman noted that in poor black neighborhoods where police raids and surveillance are constant, "young men cultivate unpredictability or altogether avoid institutions, places, and relations on which they formerly relied."[426] In one chapter, Goffman observed that the men avoided the hospital, in part because police officers habitually checked the emergency room sign-in sheet for names that might be "hot" (have outstanding warrants).[427] The men also

---

[423] HunchLab, HunchLab Academy: Overview, YouTube (Jul. 13, 2015), https://www.youtube.com/watch?v=Z-C-T2IttEs.

[424] Brayne, *supra* note 420 at 367.

[425] *See, e.g.*, WHITEHOUSE COUNCIL OF ECONOMIC ADVISERS, ISSUE BRIEF, MAPPING THE DIGITAL DIVIDE (July 2015), https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf.

[426] ALICE GOFFMAN, ON THE RUN: FUGITIVE LIFE IN AN AMERICAN CITY (2014).

[427] *Id.*

"cultivate unpredictability" by avoiding established routines and by not being where people expect them to be.[428] But is it possible to be unpredictable in a world where algorithms are constantly "learning" how to make ostensibly more reliable predictions about human behavior? The next section attempts to explore this question and to define the liberty interest in being unpredictable.

The Right to be Unpredictable

Predictive policing embodies what Danielle Citron and Frank Pasquale refer to as "the scored society."[429] In the scored society, individuals are "tagged," ranked, or rated by predictive algorithms for various purposes:

> Predictive algorithms mine personal information to make guesses about individuals' likely actions and risks. A person's on- and offline activities are turned into scores that rate them above or below others. Private and public entities rely on predictive algorithmic assessments to make important decisions about individuals.[430]

Citron and Pasquale point out that predictive algorithms can "harm individuals' life opportunities often in arbitrary and discriminatory ways."[431] In scoring, ranking, and categorizing individuals based on existing data, automated predictions threaten individual autonomy and self-determination.[432] Julie Cohen has argued that autonomy "shelters [individual experimentation, creativity, and] subjectivity from the efforts of commercial

[428] *Id.*

[429] Citron & Pasquale, *supra* note 93.

[430] *Id.* at 2–8.

[431] *Id.* at 7.

[432] *See, e.g,* Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 784–94 (1989) (defining the right to privacy as "the fundamental freedom not to have one's life too totally determined by a progressively more normalizing state. . . . [a] creeping totalitarianism, an unarmed occupation of individuals' lives. . . . The anti-totalitarian right to privacy . . . prevents the state from imposing on individuals a defined identity").

and government actors to render individuals and communities fixed, transparent, and predictable."[433] Total predictability robs individuals of the freedom to define and redefine themselves and to evolve from their pasts.

Law enforcement often insists upon the need to predict behavior in order to maintain safety and fight crime.[434] To be sure, total predictability would make fighting crime easier. But automated predictions are neither perfect nor neutral.[435] At best, even the most statistically valid predictive algorithms will create false positives, since they operate based on probabilities, not absolutes. At worst, predictive policing can encode racial and socioeconomic bias.[436] Moreover, totalitarian uses of surveillance to achieve predictability have chilling effects on expression and individualism.[437]

The unpredictability described here is not synonymous with the right to avoid crime detection. Rather, it is a general freedom to participate in society, associate with others, and develop the self without fear that innocent activities will lead to pigeonholing predictions. It protects innocent individuals, individuals for whom police have not developed reasonable suspicion, and individuals who may be labeled at-risk of committing future crimes because of social or economic circumstances. It also protects formerly convicted individuals from unfounded assumptions of recidivism. In the analog world, people can selectively cultivate unpredictability, or what Woodrow Hartzog and

---

433 Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1905 (2013).

434 *See, e.g.*, Dokoupil, *supra* note 3.

435 *See supra* Ch. IV.

436 *See supra* Ch. IV.

437 *See* Cohen, *supra* note 433, at 1912.

Evan Selinger refer to as "obscurity."[438] For example, some people leave their lights on when they're not home so that potential robbers don't learn their habits; some cross county lines to do their shopping and avoid nosy neighbors. But with algorithms that can analyze infinite amounts of data and continually adapt to new information, cultivating unpredictability or maintaining obscurity may be impossible.

The threat to liberty posed by total predictability may disparately impact the poor and communities of color, who tend to live under more persistent surveillance. For communities that are heavily surveilled, unpredictability may be a vital means of maintaining human dignity. Traditionally marginalized groups already struggle to overcome the roles and assumptions society imposes on them. Automated predictions, especially without transparency and adequate safeguards, could exacerbate the marginalization of protected groups.

Conclusion

This chapter has discussed seven potential limitations and risks associated with automated profiling. Each of these issues should be considered by the data scientists developing automated predictive policing models, by the law enforcement agencies adopting these models, and by the policymakers determining whether and how to regulate predictive policing. These actors should not stop at acknowledging these limitations or at ensuring that predictive models are reliable. Before adopting big-data law enforcement solutions, stakeholders should consider the broader social consequences of relying on statistics and machine learning to predict human behavior and inform suspicion. Over-reliance on predictive algorithms could dull officers' judgment, exacerbate existing

[438] Evan Seligner and Woodrow Hartzog, *Obscurity and Privacy*, ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY (2014).

tensions between law enforcement and communities, and chill online activity and associations. Accepting these consequences for the sake of catching more criminals would be antithetical to democratic values.

CHAPTER 5: DISCUSSION, CONCLUSIONS, AND RECOMMENDATIONS

Introduction

Automated profiling stands to fundamentally change the nature of policing and the Fourth Amendment reasonable suspicion inquiry by emphasizing the knowledge and inferences of a computer rather than those of a police officer. This chapter will summarize the findings discussed in the previous chapters and offer suggestions for how law enforcement agencies, policymakers, and software developers can minimize the civil liberties harms associated with automated profiling.

Answers to Research Questions

1. **What have courts said about if or when using profiles as a basis for investigative stops violates the Fourth Amendment? What limits have they set on these practices?**

The Fourth Amendment reasonable suspicion inquiry depends upon the specific facts observed by and known to the officer and the reasonable inferences drawn from those facts based on the officer's experience. This inquiry remains the same when those facts are drawn from a predetermined profile. Courts have generally accepted the use of predetermined profiles as a basis for investigative stops, but they have refused to give talismanic significance to any particular profile as indicating reasonable suspicion. Factors from a predetermined profile can give rise to reasonable suspicion if the specific factors relied upon, in light of the totality of the circumstances, gave rise to an officer's reasonable inference and criminal activity was afoot.

Courts disagree over whether the factors in the drug courier profile, without more, can justify reasonable suspicion. For a profile to justify reasonable suspicion, it must sufficiently narrow the pool of suspicious individuals such that it would not subject a large number of presumably innocent individuals to arbitrary seizures.

Courts also emphasize officers' training and experience, which allow officers to infer criminal activity from facially innocent behavior. A lack of experience with a particular profile or the inability to articulate one's inferences can militate against finding that an officer's inferences were reasonable.

Although no federal appellate court has rejected the drug courier profile outright, many courts have expressed skepticism about the usefulness of the profile. This skepticism often stems from the profile's malleability, the lack of proof of its statistical reliability, its tendency to lead to arbitrary seizures.

2. What major problems does automated profiling present that the existing legal frameworks do not adequately address?

The addition of machine learning to crime profiling will change the nature of the Fourth Amendment reasonable suspicion inquiry by de-emphasizing the observations and inferences of police officers. Police officers may have difficulty ascertaining and testifying to the underlying logic and facts contributing to an automated prediction. In the moment that an officer decides to act on a prediction, there are likely to be discrepancies between what the officer knows and what the predictive algorithm knows. This will alter the officer's role in the decision about whether to seize a person, which will present challenges for the Fourth Amendment reasonable suspicion inquiry, which focuses on the facts observed and known to the officer, the officer's experience, and the officer's rational inferences. Although algorithms are capable of analyzing far more information than human police officers, they are not designed to assess the totality of the circumstances in a particular moment in time, which is the crux of the reasonable suspicion inquiry. Courts may view the automated nature of automated profiling as overly formulaic and contributing to arbitrary seizures by dulling the officer's perceptions and decision-making abilities. On the other hand, courts may view the consistency and the empirical nature of automated decisions as a positive check on officer discretion that may actually limit arbitrary seizures. Automated profiling is more likely to result in "consensual" police interventions that do not fall under the Fourth Amendment's protections. However, these consensual encounters may still evolve into seizures. Automated predictions may not have the same degree of temporal exigency as typical law enforcement decisions to perform *Terry* stops. Automated predictions are designed to indicate that someone will commit a crime at some point in the future, but they do not necessarily indicate that someone is committing or is about to commit a crime—the current standard for reasonable suspicion.

3. **What limitations and policy considerations should data scientists, law enforcement agencies, and policymakers consider before designing, implementing, and regulating automated profiling models?**

Automated predictive models are not inherently neutral. Many factors, including unreliable data, human subjectivity, and oversensitivity, can compromise the relevance and reliability of predictive models, which can lead to discrimination and can compromise civil liberties. Automated predictive models are designed to be much more sensitive to associational patterns than humans are. This can lead predictive models to find statistical associations that are not particularly probative of crime and should not be considered relevant factors in decisions about whether to investigate an individual. However, predictive models may actually overstate the relevance of these connections if they are not carefully calibrated. It is difficult to come up with a reliable sample of crime data. Crime data are limited to instances where criminals "got caught;" law enforcement has been historically inconsistent in its data collection and recordkeeping practices, and serious crimes are "infrequent events," which create smaller and less reliable samples. The use of commercially available digital data exacerbates this problem, since such datasets tend to be incomplete. Predictive models may be difficult to falsify because their goal is to predict and alter the future by preventing crimes and because they can cause self-fulfilling prophecies by focusing police attention on particular individuals. Predictive models can encode individual and societal biases, which can lead to discrimination against minority groups that is difficult to detect. The private ownership of predictive algorithms, as well as the inherently opaque nature of machine learning, can frustrate government openness. Predictive policing encourages a law enforcement culture characterized by an over-reliance on statistics and crime control at the expense of holistic protection of legal rights and democratic values. Overreliance on automated predictions may also exacerbate the phenomenon of system avoidance that disproportionately discourages poor and black individuals from participating in social institutions.

4. **How can some of the problems identified in the answers to research questions two and three be addressed?**

The following section answers this question by reflecting on the foregoing research and offering practical principles for adopting, using, and regulating automated profiling in ways that reduce potential harm.

Conclusions and Guidelines for Minimizing the Potential Harms Associated with Automated Profiling

The term "hot" is used colloquially to describe people who may be in trouble with the law. Traditionally, this includes people with outstanding arrest warrants, people who are carrying contraband, or people who have been involved in an unsolved crime. "Hot" people are those who have a tangible reason to fear that, if identified by police, they will be arrested. Predictive policing is changing what it means to be hot by increasing the scope of information—and the capabilities to process it—that can lead to an individual being targeted for investigation. As algorithms attempt to predict crimes well in advance of a criminal act, the facts that form the basis of suspicion will be necessarily attenuated from the crime itself. Automated predictive software may make it easier for police to predict crime. At the same time, these tools will make it harder for individuals to predict whether they are hot. The law enforcement community would argue—perhaps justifiably—that this is a good thing. This one-way predictability will make it easier for police to catch criminals while making it harder for criminals to evade police. But it also means that anyone—innocent or not—can become the subject of suspicion for reasons beyond his or her control. The comforting maxim that those who have nothing to hide have nothing to fear no longer applies. This leaves individuals to worry that their otherwise innocent activities—particularly those conducted or recorded online—will subject them to police scrutiny and possibly even arrest by marking them as a probabilistic criminal. This could have chilling effects on online and offline conduct, particularly on speech and associational activities. These effects will likely be concentrated among low-income and black individuals, who are already more likely to be stopped by police and arrested.

Given that the statistical science of automated crime prediction is in its infancy, the current benefits of automated profiling may not be worth the risks to civil liberties. It would behoove law enforcement and government agencies to carefully consider these tradeoffs before implementing predictive policing programs. Nonetheless, law enforcement agencies across the country have already adopted some of these tools and are deploying them in communities. The following is a list of recommendations for minimizing the harms associated with automated profiling. This is not meant to be a comprehensive list of guidelines for predictive policing. It is merely a modest answer to some of the problems this thesis has documented.

1. Before developing predictive software, data scientists should seek to answer whether a particular type of crime can be reliably predicted. Some types of crime may lack adequate data or patterns to support reliable predictions, as in McCue's example of armed robberies that escalate into aggravated assaults. Since infrequent events create smaller and less reliable sample datasets, attempting to predict rare crimes may be more harmful than helpful.

2. Automated predictions should provide officers with as much underlying information as possible in a useful format. The prediction should provide not only the what (the crime likely to occur) or the who (the likely suspect) but also the why. It should tell the police officer which factors or characteristics indicate that an individual is at risk

of committing a crime. This can allow the officer to better evaluate the usefulness of the prediction given the totality of the circumstances.

3. Police officers should engage carefully with predictions and question their accuracy and usefulness, rather than taking them at face value. Although algorithms can analyze information in ways that the human brain cannot, police officers are in a better position to assess whether the circumstances surrounding a prediction warrant an intervention. Thus, policies that call for officers to act on every prediction—such as Chicago's Custom Notifications program—are unwise. Automated predictions should not completely supersede or dictate officers' judgment.

4. Before any data are entered into an automated prediction system, their reliability should be verified by experts. At least one automated predictive policing system, Hunchlab, currently claims that officers can input any dataset they want into the system and that Hunchlab will decide how to process the data. However, it is unclear whether and how these datasets would be subjected to reliability tests and controls or "scrubbing." Programmers and officers should work together to determine which datasets to input into predictive software, the reliability of those datasets, and how to treat the information.

5. The law enforcement community should not take for granted that all non-Fourth Amendment police-citizen encounters are benign or beneficial. Fourth Amendment law treats these encounters as negligible encroachments upon liberty interests, and predictive policing programs that emphasize intervention suggest that such encounters can be beneficial. However, even low-level police intervention can have chilling consequences, discouraging individuals from interacting with recordkeeping

institutions for fear that they are being surveilled. Home visits, such as those recommended by Chicago's Custom Notifications program, should not be taken lightly.

6. Law enforcement agencies should provide information to the public about which predictive systems they are using, how they are using them, how the systems operate, and any rules or guidelines they follow when using the systems. Transparency regarding predictive systems and practices is an important prerequisite to public trust in law enforcement.

7. When prediction-based seizures are challenged, courts should require officers to testify to the prediction's underlying justification—including the criteria giving rise to the prediction—in open court, and the record of this testimony should be publicly available. The requirement that officers articulate the facts giving rise to reasonable suspicion has provided the public, as well as attorneys and judges, with a record showing which circumstances gave rise to reasonable suspicion and which circumstances fell short of this standard. If the facts and reasoning underlying automated predictions are allowed to remain under seal, this important record—a mechanism for keeping legal institutions accountable—will be lost.

Questions for Further Research

Because little is publicly known about the algorithms and data used in predictive policing models and the policies police follow when using them, future research should attempt to discover and discuss these details. Computer science experts should weigh in on the existence of reliable methods of ensuring that automated profiling models and the data they use don't create predictions that consider race, economic status, or other improper factors, including proxies for these characteristics.

REFERENCES

ACLU OF ILLINOIS, STOP AND FRISK IN CHICAGO (March 2015), http://www.aclu-il.org/wp-content/uploads/2015/03/ACLU_StopandFrisk_6.pdf.

Sameer Bajaj, Note, *Policing the Fourth Amendment: the Constitutionality of Warrantless Investigatory Stops for Past Misdemeanors*, 109 COLUM. L. REV. 309 (2009).

Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. __, 6–7 (forthcoming 2016).

Anna Maria Barry-Jester et al., *The New Science of Sentencing*, THE MARSHALL PROJECT (Aug. 4, 2015), https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing.

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.

Nathaniel Bronstein, *Police Management and Quotas: Governance in the CompStat Era*, 48 COLUM. J.L. & SOC. PROBS. 543 (2015).

Danielle Keats Citron, *Data Mining for Juvenile Offenders*, CONCURRING OPINIONS (Apr. 21, 2010, 3:56 PM), http://concurringopinions.com/archives/2010/04/data-mining-for-juvenile-offenders.html.

Danielle Keats Citron, *Technological Due Process*, 85 WASH. L. REV. 1249 (2008).

Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014).

CIVIL RIGHTS, BIG DATA, AND OUR ALGORITHMIC FUTURE (September 2014), https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-Algorithmic-Future-v1.2.pdf.

Morgan Cloud, *Search and Seizure by the Numbers: The Drug Courier Profile and Judicial Review of Investigative Formulas*, 65 B. U. L. Rev. 843 (1985).

Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904 (2013).

David Cole, *Discretion and Discrimination Reconsidered: A Response to the New Criminal Justice Scholarship*, 87 GEO. L. J. 1059 (1999).

E. GABRIELLA COLEMAN, CODING FREEDOM (2013).

COMMITTEE ON THE ANALYSIS OF MASSIVE DATA, ET AL., FRONTIERS IN MASSIVE DATA ANALYSIS (2013), http://bigdatawg.nist.gov/FrontiersInMassiveDataAnalysisPrepub.pdf.

Joshua Correll, et al., *Across the Thin Blue Line: Police Officers and Racial Bias in the Decision to Shoot*, 92 J. PERSONALITY & SOC. PSYCH. 1006 (2007).

Kate Crawford, *Think Again: Big Data*, FOREIGN POL'Y (May 10, 2013), http://foreignpolicy.com/2013/05/10/think-again-big-data/.

David Curry, Richard A. Ball, & Robert J. Fox, *Gang Crime and Law Enforcement Recordkeeping*, NIJ RESEARCH IN BRIEF (1994), https://www.ncjrs.gov/txtfiles/gcrime.txt.

Angela J. Davis, *Race, Cops, and Traffic Stops*, 51 U. MIAMI L. REV. 425 (1997).

Tony Dokoupil, *'Small World of Murder': A Homicides Drop, Chicago Police Focus on Social Networks of Gangs*, NBC NEWS, http://www.nbcnews.com/news/other/small-world-murder-homicides-drop-chicago-police-focus-social-networks-f2D11758025.

John Eligon & 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.

Steven J. Ellwanger, Predictive Policing 698, *in* ENCYCLOPEDIA OF CRIMINAL JUSTICE ETHICS (Bruce A. Arrigo, ed. 2014).

Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015).

Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L. J. 259 (2012).

Andrew Guthrie Ferguson & Damien Bernache, *The "High-Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment Reasonable Suspicion Analysis*, 57 AM. U. L. REV. 1587 (2008).

ALICE GOFFMAN, ON THE RUN: FUGITIVE LIFE IN AN AMERICAN CITY (2014).

Erica Goode, *Sending the Police Before There's a Crime*, New York Times (Aug. 15, 2011), http://www.nytimes.com/2011/08/16/us/16police.html.

Samuel R. Gross & Debra Livingston, *Racial Profiling Under Attack*, 102 COLUM. L. REV. 1413 (2002).

Peter Hanink, *Don't Trust the Police: Stop Question and Frisk, CompStat, and the High Cost of Statistical Over-Reliance in the NYPD*, J. INST. JUSTICE & INT'L STUDIES 99 (2013).

David A. Harris, *Factors for Reasonable Suspicion: When Black and Poor Means Stopped and Frisked*, 69 IND. L.J. 659 (1994).

VINCENT E. HENRY, THE COMPSTAT PARADIGM: MANAGEMENT ACCOUNTABILITY IN POLICING, BUSINESS AND THE PUBLIC SECTOR (2003).

Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2015).

US: Drug Arrests Skewed by Race, HUMAN RIGHTS WATCH (Mar. 2, 2009), https://www.hrw.org/news/2009/03/02/us-drug-arrests-skewed-race.

Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 Harv. L. & Pol'y Rev. 15 (2016).

Elizabeth E. Joh, *Policing By Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014).

Sheri Lynn Johnson, *Race and the Decision to Detain a Suspect*, 93 YALE L.J. 214 (1983).

Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score'*, WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.

Lewis R. Katz, Terry v. Ohio *at Thirty-Five: A Revisionist View*, 74 MISS. L.J. 423 (2004).

Alexander H. Kipperman, Note and Comment, *Frisky Business: Mitigating Predictive Crime Software's Facilitation of Unlawful Stop and Frisks*, 24 TEMP. POL. & CIV. RTS. L. REV. 215 (2014).

Gary Kleck, *Racial Discrimination in Criminal Sentencing: A Critical Evaluation of the Evidence with Additional Evidence on the Death Penalty*, 46 AM. SOC. REV. 783 (1981).

WAYNE R. LAFAVE ET AL., 2 CRIMINAL PROCEDURE (3d ed. 2014).

Wayne R. LaFave, *Controlling Discretion by Administrative Regulations: The Use, Misuse, and Nonuse of Police Rules and Policies in Fourth Amendment Adjudication*, 89 MICH. L. REV. 442 (1990).

Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L. REV. 1 (1994).

Alice E. Marwick, *How Your Data are Being Deeply Mined*, N.Y. REV. BOOKS (Jan. 9, 2014), http://www.nybooks.com/articles/2014/01/09/how-your-data-are-being-deeply-mined/.

GARRY F. MCCARTHY, CUSTOM NOTIFICATIONS IN CHICAGO – PILOT PROGRAM D13-09, http://directives.chicagopolice.org/directives-mobile/data/a7a57bf0-13fa59ed-26113-fa63-2e1d9a10bb60b9ae.html?ownapi=1.

COLLEEN MCCUE, DATA MINING AND PREDICTIVE ANALYSIS: INTELLIGENCE GATHERING AND CRIME ANALYSIS (2006).

Deborah L. Meyer, *The Spot Program: Hello Racial Profiling, Goodbye Fourth Amendment*, 10 U. MD. L.J. 289 (2010).

Richard E. Myers II, *Challenges to* Terry *for the Twenty-First Century*, 81 MISS. L. J. 937 (2012).

New York Times, Cities for Tomorrow, *Data Mining and the Modern City* (2015), http://nytcitiesfortomorrow.com/gallery/cities-for-tomorrow-2016/2015-videos/1517.

JEFFREY S. PAUL & THOMAS M. JOINER, INTEGRATION OF CENTRALIZED INTELLIGENCE WITH GEOGRAPHIC INFORMATION SYSTEMS: A COUNTYWIDE INITIATIVE, GEOGRAPHY & PUB. SAFETY (2011).

Dana Raigrodski, *Reasonableness and Objectivity: A Feminist Discourse of the Fourth Amendment*, 17 TEX. J. WOMEN & L. 153 (2008).

David Robinson, *Buyer Beware: A Hard Look at Police 'Threat Scores'*, EQUALFUTURE (Jan. 14, 2016), https://www.equalfuture.us/2016/01/14/buyer-beware-police-threat-scores/.

Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989).

Evan Seligner & Woodrow Hartzog, *Obscurity and Privacy*, ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY (2014).

KATHLEEN SHORT, U.S. CENSUS BUREAU, THE SUPPLEMENTAL POVERTY MEASURE (2014).

HARVEY A. SILVERGLATE, THREE FELONIES A DAY: HOW THE FEDS TARGET THE INNOCENT (2009).

ELI B. SILVERMAN, NYPD BATTLES CRIME: INNOVATIVE STRATEGIES IN POLICING (1999).

David A. Slansky, *Traffic Stops, Minority Motorists, and the Future of the Fourth Amendment*, 1997 SUP. CT. REV. 271 (1997).

Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1 (1991).

Jay Stanley, *Chicago Police "Heat List" Renews Old Fears About Government Flagging and Tagging*, AM. CIVIL LIBERTIES UNION: FREE FUTURE BLOG (Feb, 25, 2014), https://www.aclu.org/blog/chicago-police-heat-list-renews-old-fears-about-government-flagging-and-tagging.

William J. Stuntz, *Race, Class, and Drugs*, 98 COLUM. L. REV. 1795 (1998).

Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87 (2014).

Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMMS. OF THE ACM 44 (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240&download=yes.

Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956 (1999).

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/#442d97b26931.

U.S. DEP'T OF JUSTICE, POLICE BEHAVIOR DURING TRAFFIC AND STREET STOPS, 2011 (Sept. 2013), http://www.bjs.gov/content/pub/pdf/pbtss11.pdf.

DAVID WEISBURD, ET AL., POLICE FOUNDATION REPORTS, THE GROWTH OF COMPSTAT IN AMERICAN POLICING (2004), http://assets.lapdonline.org/assets/pdf/growthofcompstat.pdf.

WHITEHOUSE COUNCIL OF ECONOMIC ADVISERS, ISSUE BRIEF, MAPPING THE DIGITAL DIVIDE (July 2015), https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf.

Gregory Howard Williams, *The Supreme Court and Broken Promises: The Gradual But Continual Erosion of* Terry v. Ohio, 34 HOW. L. J. 467 (1991).

Colin D. Wood, *They Didn't Look Right to Me!: Reasonable Suspicion in Kansas: Through Whose Eyes Is It Viewed?*, 76 J. KAN. B.A. 16 (2007).