REASONABLY SUSPICIOUS ALGORITHMS: PREDICTIVE POLICING AT THE UNITED STATES BORDER

LINDSEY BARRETT[∞]

ABSTRACT

As big data's promises of increased efficiency and serendipitous insights spread across a broad range of sectors, they are accompanied by new risks—some intuitive, some unpredictable. That dichotomy is heavily accentuated in the law enforcement context, where blithe application of new technologies to analogue doctrines poses a greater threat to individual rights. The potential for data analytics to add efficiency, accuracy, and accountability to existing procedures could be all the more beneficial. Predictive policing algorithms, which approximate the probability of crimes occurring in certain areas, or being committed by certain people, epitomize this dual dynamic. These algorithms have the potential to increase accuracy and efficiency, but they also threaten to dilute the reasonable suspicion standard and increase unintentional discrimination in a way that existing law is ill-equipped to prevent. This threat is of particular concern at the United States border. At the border, Fourth Amendment protections are generally weaker than in the interior due to the long-recognized governmental prerogative to investigate external threats poised to infiltrate the country. This article will argue that the use of predictive policing algorithms at the border should not be barred outright, as the government should permit potentially beneficial uses of the technology to develop. However, use of these algorithms should be carefully limited by statute to prevent the wholesale trammeling of privacy and civil liberties.

[∞] B.A., 2014, Duke University; J.D. 2017, Georgetown University Law Center. Many thanks to Professor David Vladeck, Professor Julie Cohen, Margaret O'Malley, Lawrence Byrne, and Arjun Sethi for their invaluable guidance; and an enormous thank you to Professor Paul Ohm, without whose inexhaustible patience and insightful feedback this Article would not have been possible.

I.
INTRODUCTION

Data analytics is increasingly a part of the way society operates: the brave new world is becoming the norm. In every sector, the oracular magic of big data seems to offer unimaginable insights, and new ways to increase efficiency while lowering costs. But new solutions tend to create new problems, which is of particular concern when those problems are ill-understood, or seemingly innocuous enough to go ignored. The use of big data in law enforcement further raises those stakes: the objectives are more significant, and the potential errors more consequential. Predictive policing algorithms, which use a variety of data to predict the probability of crimes being committed in certain areas, or by certain people, contain that dual potential for enormous benefits, coupled with considerable risks.

While legal scholars have examined the impact of the border context on the Fourth Amendment,[1] the implications of predictive policing programs for that Amendment,[2] and the implications of predictive and scoring algorithms for

1. *See generally* Jon Adams, *Rights at United States Borders*, 19 BYU J. PUB. L. 353 (2005) (discussing the Fourth Amendment border exception).

2. *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 388 (2015) [hereinafter Ferguson, *Big Data*] (comparing the use of vast amounts of networked data with prior investigative techniques in formulating a judgment of reasonable suspicion); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 285–89 (2012) [hereinafter Ferguson, *Predictive Policing*] (discussing different predictive policing tools and the possible privacy risks that may accompany their development).

substantive and procedural due process outside of the criminal context,[3] there has been relatively little written about the use of predictive policing in the border context. Employing predictive algorithms poses risks to privacy and civil liberties in the criminal context generally, but poses an even greater risk in contexts where existing legal safeguards offer less protection. The threat is particularly severe at the border, where longstanding norms have dictated weaker Fourth Amendment protections, reflecting the government's heightened prerogative to investigate external threats.[4] However, none of the determinations produced by predictive policing programs rise to the legal standard of a Fourth Amendment search or seizure, so their use by the police does not require probable cause or a warrant. And while predictive policing techniques are analogous to existing portions of the reasonable suspicion doctrine, such as police reliance on informant tips, profiling, and the assessment of a particular area as "high-crime," the technology creates distinct concerns that courts are unlikely to recognize or address, and with which the Fourth Amendment is ill-equipped to grapple. Substituting often biased or otherwise flawed algorithmic predictions for prior investigative techniques risks skewing the judgment of law enforcement officials, resulting in arbitrary and discriminatory stops, searches, and arrests, and a likely dilution of the reasonable suspicion standard.

Ultimately, the Fourth Amendment is unlikely to provide sufficient safeguards against the kinds of harms predictive policing technology will produce in the border context. The resulting choices are to adjust the reasonable suspicion standard to account for the use of predictive policing; categorically prohibit the use of the technology; or establish careful statutory safeguards to limit its impact. A different judicial approach to analyzing reasonable suspicion at the border would contradict the longstanding precedent of deference to governmental prerogatives in that context, a jurisprudential leap that the courts are unlikely to find remotely tenable.[5] Even if categorical bans against the technology were

3. *See generally* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (asserting the need for due process protections for the use of algorithmically generated risk assessments, such as financial risk indicators); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008) (maintaining that the inevitable lapses inherent in translating policy into code compel individual due process protections to accompany automated decisionmaking); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014) (arguing for a procedural due process right to protect individual privacy due to the pervasive use of predictive data analytics).

4. United States v. Ramsey, 431 U.S. 606, 616 (1977) (establishing the border exception to the Fourth Amendment in asserting that searches made at the border "are reasonable simply by virtue of the fact that they occur at the border").

5. Ferguson, *Big Data*, *supra* note 2, at 405 (discussing how the use of big data is inapposite for reasonable suspicion doctrines predicated on the use of more limited information, and noting that while one solution could be to change the reasonable suspicion standard, "[t]he Supreme Court has been steadfast in articulating that it has no intention of quantifying—or even clarifying—the standard, instead recognizing that police officers operate within 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act'") (quoting Illinois v. Gates, 462 U.S. 213, 231 (1983)).

politically feasible or normatively advisable, they would stymie development of the technology. If designed well, predictive policing programs could be used to limit discriminatory police activity rather than advance it, while also increasing overall efficiency and effectiveness. Broad prohibition is an extreme remedy to a problem that requires a carefully tailored approach; thoughtful safeguards could allow law enforcement to harness the benefits of predictive policing while tempering the potential risks.

This article argues that the use of predictive policing programs should be limited, but not banned, in the border context. The technology is ostensibly compatible with previous techniques used in reasonable suspicion doctrine, but is more likely to deliver incorrect or biased predictions. The use of biased or otherwise flawed predictions will result in discriminatory and arbitrary law policing at the border, in part by diluting the reasonable suspicion standard, due to the perception that the predictions are neutral, and interchangeable with prior methods, when they are in fact fairly flawed. Part II provides a background on the Fourth Amendment, the reasonable suspicion standard, and how those doctrines operate in the border context. Part III explains predictive policing algorithms and the application of the Fourth Amendment to their use. Part IV uses two hypotheticals to demonstrate the apparent similarity between predictive policing and the reasonable suspicion standard, and to illustrate how predictive policing possesses the potential to dilute that standard. Part V explores the flaws in predictive policing software that are likely to weaken what few privacy and civil liberties protections remain at the border, looking particularly at automation bias, the potential for discriminatory impact, and lack of transparency. The Article concludes by proposing statutory limits on the use of predictive policing that encourage development and implementation of the technology in a way that protects privacy and civil liberties. Predictive policing cannot and should not be implemented without rigorous safeguards, but neither should its potential to improve law enforcement methods go wholly ignored.

II.
THE FOURTH AMENDMENT

A. The Fourth Amendment in the Interior

The Constitution protects the right of individuals to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[6] This standard affords individuals a subjectively reasonable expectation of privacy that society is prepared to recognize as objectively reasonable.[7] In the interior of the United States, i.e., any geographical location that is not the border, the standard

6. U.S. CONST. amend. IV.

7. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (establishing the reasonable expectation of privacy test).

generally requires probable cause or a warrant for any search or seizure.[8] Probable cause does not, however, require mathematical specificity,[9] and there are a number of exceptions to the warrant requirement.

In *Terry v. Ohio*, the Supreme Court recognized a form of investigative intrusion by the police that does not rise to the level of a Fourth Amendment search, but is still governed by the reasonableness requirement of the Amendment.[10] When an officer has reasonable suspicion—more than a "hunch" but less than probable cause[11]—that criminal activity is occurring or will imminently occur, she may briefly stop, detain, and question that person if the suspicion is supported by articulable facts that are particularized to the defendant.[12] Those facts and the rational inferences from them must reasonably justify the intrusion, and must be proportionate to the scope of the intrusion.[13]

The calculus of reasonable suspicion is determined in light of the totality of the circumstances,[14] as opposed to the retroactive parsing of individual factors, and one factor alone is not determinative.[15] Facts that may be individually innocuous may nevertheless suffice in aggregate,[16] and the judgment of whether ostensibly innocent facts create a collective presumption of reasonable suspicion is left to the officer's expertise.[17] The totality of circumstances test also takes account of factors weighing for and against reasonable suspicion—a flexible standard that gives credence to officer's experience and allows for discretion in considering a wide range of factors.[18] But the "virtue of flexibility" brings with it

8. *See, e.g.*, United States v. Ross, 456 U.S. 798, 824–25 (1982) (quoting Mincey v. Arizona, 437 U.S. 385, 390 (1978)).

9. *See* Illinois v. Gates, 462 U.S. 213, 245 n.14 (1983) ("We have never required that informants used by the police be infallible, and can see no reason to impose such a requirement in this case. Probable cause, particularly when police have obtained a warrant, simply does not require the perfection the dissent finds necessary.").

10. *See* Terry v. Ohio, 392 U.S. 1, 30–31 (1968).

11. *See* United States v. Arvizu, 534 U.S. 266, 274–78 (2002); *Terry*, 392 U.S. at 27.

12. *See Terry*, 392 U.S. at 27.

13. *Id.* at 19 ("The scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible.") (Fortas J., concurring) (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967)).

14. United States v. Cortez, 449 U.S. 411, 417 (1981).

15. *See* United States v. Zapata-Ibarra, 212 F.3d 877, 881 (5th Cir. 2000).

16. United States v. Sokolow, 490 U.S. 1, 9 (1989).

17. *See* United States v. Arvizu, 534 U.S. 266, 275–76 (2002) ("We think it quite reasonable that a driver's slowing down, stiffening of posture, and failure to acknowledge a sighted law enforcement officer might well be unremarkable in one instance (such as a busy San Francisco highway) while quite unusual in another (such as a remote portion of rural southeastern Arizona).").

18. *See* United States v. Brignoni-Ponce, 422 U.S. 873, 884 (1975) ("Any number of factors may be taken into account in deciding whether there is reasonable suspicion to stop a car in the border area."); *see also* Samuel A. Townsend, *Laptop Searches at the Border and* United States v. Cotterman, 94 B.U. L. REV. 1745, 1749–50 (2014) (discussing critiques of "the unclear and flexible nature of reasonable suspicion," which "caused some to criticize the standard, including Justice Thurgood Marshall").

the "vice of malleability,"[19] and that malleability is put to a particularly rigorous test in the Fourth Amendment jurisprudence governing searches and seizures conducted at the U.S. border.

B. The Fourth Amendment at the Border

Since the beginning of the Republic, courts have recognized the heightened prerogative of the sovereign to investigate persons or cargoes seeking to enter the territory from the exterior.[20] Stops and searches that occur at an international border or its functional equivalent fall under the Fourth Amendment category of administrative or "special needs"[21] searches, in which a particular need for government efficiency merits more generous accommodation than in other circumstances.[22] The constitutionality of an administrative search depends on (1) the significance of the public concerns served (here, the government interest); (2) the extent to which a warrantless search advances the public interest; and (3) the severity of the interference with individual liberty or privacy.[23] In the border context, this calculus is heavily tilted towards the government interest. The Supreme Court characterizes such intrusions as routine stops, searches, and seizures—which do not require the government have any reasonable suspicion whatsoever—as opposed to non-routine searches and seizures, which do require reasonable suspicion.[24] The Supreme Court has refused to set a categorical threshold establishing definitive criteria for when searches and seizures at the border are non-routine, but has identified three circumstances which might trigger a reasonable suspicion requirement: (1) "highly intrusive searches of the person;" (2) destructive searches of property; and (3) searches conducted in a "particularly offensive" manner.[25] Any search less intrusive is considered reasonable by virtue

19. Ferguson, *Big Data*, *supra* note 2, at 340.

20. United States v. Ramsey, 431 U.S. 606, 616 (1977).

21. Abidor v. Napolitano, 990 F. Supp. 2d 260, 279 (E.D.N.Y. 2013).

22. *Id*. at 264 (citing United States v. Flores-Montano, 541 U.S. 149 (2004)).

23. Brown v. Texas, 443 U.S. 47, 50–51 (1979) (establishing the three-prong test for special needs searches).

24. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("[T]he Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . .") (citing United States v. Ramsey, 431 U.S. 606, 616–17, (1977)); *Id*. at 541 n.4 ("[W]e suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches."); *see also* Thomas Mann Miller, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943, 1959–60 ("Examples of nonroutine searches requiring reasonable suspicion include strip searches, alimentary canal searches, x-rays, and removal of an artificial limb. In practice, at least in reported cases, the government has demonstrated significant evidence before conducting such intrusive body searches: 'It is fair to say that most of the reported cases upholding body cavity border searches have in fact involved rather strong evidence that smuggled goods were being carried in a body cavity.'") (internal citations omitted).

25. United States v. Cotterman, 709 F.3d 952, 973 (9th Cir. 2013) (Callahan, J., concurring) (citing *Flores-Montano*, 541 U.S. at 152–56, 155 n.2).

of the fact that it occurs at the border, though further investigation could render the stop non-routine, such that some degree of Fourth Amendment protections would then apply.[26] The Supreme Court has left open the question of "whether, and under what circumstances, a border search of a vehicle might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out,"[27] though previously cited hallmark intrusive searches include strip searches, body cavity searches, and involuntary x-rays.[28]

Though non-routine searches do require a certain degree of individualized, particularized suspicion, the Supreme Court has refused to establish the precise contours of that standard.[29] The extensive list of factors an officer may take into account,[30] defined broadly in *United States v. Brignoni-Ponce*[31] is often self-contradictory,[32] allowing for nearly any set of circumstances to be construed as creating reasonable suspicion of criminal activity. The Court in *Brignoni-Ponce* listed the non-exhaustive set of factors as the characteristics about the area where the search is occurring, proximity to the border, aspects of the vehicle being searched, the number of passengers, and the behavior and appearance of the driver, which may include the "characteristic appearance of persons who live in Mexico."[33] While insufficient as the sole basis of suspicion, the apparent ancestry or physical characteristics of a suspect constitute legally sufficient criteria in

26. United States v. Ramsey, 431 U.S. 606, 616 (1977); *Flores-Montano*, 541 U.S. at 155 n.2 ("We again leave open the question 'whether, and under what circumstances, a border search might be deemed "unreasonable" because of the particularly offensive manner in which it is carried out.'") (citing *Ramsey*, 431 U.S. at 618 n.13).

27. *Flores-Montano* at 155 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13).

28. United States v. Montoya de Hernandez, 473 U.S. 531, 541 n.4 (1985).

29. *Id*. ("[W]e suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches.").

30. Adams, *supra* note 1, at 364–65 (listing twelve factors which may be taken into account for determining reasonableness, including excessive nervousness, unusual conduct, an informant's tip, computerized information showing pertinent criminal propensities, loose-fitting or bulky clothing, lack of employment or a claim of self-employment, needle marks or other indications of drug addiction, inadequate luggage, and evasive or contradictory answers, among others); United States v. Garza, 727 F.3d 436, 443 n.3 (5th Cir. 2013) (Elrod, J., dissenting) ("Our precedent is inconsistent regarding the impact of allegedly 'nervous' behavior."); United States v. Zapata-Ibarra, 223 F.3d 281, 282–83 (5th Cir. 2000) (Wiener, J., dissenting) (describing 10 sets of contradictory factors that have been found to comprise reasonable suspicion at the border).

31. United States v. Brignoni-Ponce, 422 U.S. 873, 884–85 (1975) ("Officers may consider the characteristics of the area in which they encounter a vehicle. Its proximity to the border, the usual patterns of traffic on the particular road, and previous experience with alien traffic are all relevant.").

32. By "self-contradictory," I mean that the presence of one factor in a case can create a reasonable suspicion whereas the absence of that factor in another case could also create a reasonable suspicion. The combination of an encyclopedic list of factors and a permissive standard have produced the result that factors that have been deemed as innocuous in one context can be deemed indicative of malfeasance in another. Judge Wiener, for example, describes how the fact that a car being "suspiciously dirty and muddy" has been cited as creating a reasonable suspicion, but so too has the contradictory fact of a car being "suspiciously squeaky-clean." *Zapata-Ibarra*, 223 F.3d at 282.

33. *Brignoni-Ponce*, 422 U.S. at 885.

establishing reasonable suspicion as to whether a suspect is or is harboring an illegal alien.[34]

Reasonable suspicion does not require all the *Brignoni-Ponce* factors to be met, or for the officer to eliminate all innocuous justifications for the conduct.[35] In *United States v. Martinez-Fuerte*,[36] the Supreme Court held that government officials could stop vehicles at established checkpoints for brief questioning and refer the vehicle and its occupants to a secondary checkpoint for further questioning without the existence of individualized suspicion, even though further detention or search requires consent or probable cause.[37] The court's repeated refusal to establish a "neat set of rules"[38] or parse the experienced judgment of an officer by engaging in a post-hoc "divide and conquer"[39] analysis of each factor isolated from the totality of the circumstances creates a broad standard designed to accommodate the gamut of fact-specific circumstances. However, the same standard that is designed to avoid unduly hampering law enforcement is susceptible to manipulation. The significant deference courts grant the government in Fourth Amendment analysis at the border,[40] coupled with the self-contradicting list of factors that can render a search reasonable, can result in arbitrary enforcement.

III.
PREDICTIVE POLICING

A. Defining "Predictive Policing"

The premise of predictive policing software—that police can more accurately and efficiently prevent crime based on prior patterns—is nothing new. At its heart, predictive policing is the data-driven incarnation of what criminological theories have been attempting for decades: to analyze past events, infer broader patterns, and then use those insights to prevent crime. "Predictive policing" encompasses the use of data analysis and criminological theories in predictive models.[41] Using

34. *Id*. at 886–87 ("The likelihood that any given person of Mexican ancestry is an alien is high enough to make Mexican appearance a relevant factor, but standing alone it does not justify stopping all Mexican-Americans to ask if they are aliens.").

35. *Zapata-Ibarra*, 212 F.3d at 884.

36. United States v. Martinez-Fuerte, 428 U.S. 543, 563 (1976).

37. *Id*.

38. United States v. Arvizu, 534 U.S. 266, 274 (2002).

39. *Id*.

40. United States v. Zapata-Ibarra, 223 F.3d 281, 281 (5th Cir. 2000) (Weiner, J., dissenting) (lambasting the federal judiciary for having "placed the Fourth Amendment's protection of 'the people' from unreasonable searches and seizures into a state of suspended animation anywhere even remotely close to the Mexican border."); *see also* Janet C. Hoeffel & Stephen Singer, *Fear and Loathing at the U.S. Border*, 82 MISS. L.J. 833, 840 (2013) (arguing that if the border search doctrine "were treated as the administrative search that it is, the courts would scrutinize and likely condemn the extraordinary breadth of discretion and potential for abuse of that discretion by border officials").

41. Ferguson, *Predictive Policing*, *supra* note 2, at 265.

certain factors, these models can approximate who will commit crimes and where they will commit them.[42] The key difference between applying criminological theories to policing techniques, and implementing those theories into algorithms, is the purifying aura of empirical accuracy that data analysis claims to confer. In reality, however, an algorithm is only as infallible as the human beings who choose the variables, input the data, and act on the results.

Different models have distinct Fourth Amendment analogues and differing implications for individual rights. The four basic models can be categorized as methods for predicting (1) crimes; (2) offenders; (3) perpetrator identities; and 4) crime victims.[43] The first two models are the most relevant in the border context, where the primary mission is to prevent future crimes in a specific area—the U.S. border—and to determine the status of the individuals crossing it. The following section will provide context on the development of predictive policing software, including three of the most widely used commercially available technologies: PredPol and HunchLab (both area-based predictions), and Beware (individualized risk assessments of potential offenders). PredPol relies on hot-spot mapping, a geographical approach to crime analysis predicated on the fact that crime is not evenly dispersed,[44] and near-repeat theory, which attempts to explain why hotspots continue to experience more criminal activity than other areas.[45] HunchLab uses a broader array of factors and risk terrain modeling. Beware generates individualized threat scores from publicly available data sources. These programs use public arrest records, social media posts, and information compiled by commercial data brokers to assess the relative risk of an individual committing a crime.

B. Area-Based Predictions and Individualized Risk Assessments

The basic premise that crime is not evenly dispersed geographically has been widely accepted, giving rise to the technique of hotspot mapping. Hotspot mapping identifies areas with high incidences of crime on the assumption that those areas are more likely to experience a higher incidence of crime for a certain period of time than are other areas.[46] With traditional hotspot mapping, police officers would plot the occurrence of crime on a map, and direct additional police officers to those areas.[47] Programs like PredPol use historical crime data to

42. *Id*. at 265–67.

43. WALTER L. PERRY, BRIAN MCINNIS, CARTER C. PRICE, SUSAN C. SMITH & JOHN S. HOLLYWOOD, RAND CORPORATION, PREDICTIVE POLICING: THE ROLE OF CRIME FORECASTING IN LAW ENFORCEMENT OPERATIONS 8 (2013) [hereinafter RAND REPORT], http://www.rand.org/pubs/research_reports/RR233.html [https://perma.cc/DXD8-4UP8].

44. Ferguson, *Predictive Policing*, *supra* note 2, at 273.

45. *Id*. at 277.

46. *Id*. at 273.

47. RAND REPORT, *supra* note 43, at xvii ("Making 'predictions' is only half of prediction-led policing; the other half is carrying out interventions, acting on the predictions that lead to reduced crime (or at least solve crimes).").

calculate the probability of particular crimes happening in a given area over a period of time. A high probability automates the creation of a hotspot. PredPol relies solely on historical crime data in conjunction with near-repeat theory, which posits that certain crimes occur in close temporal and spatial windows to where they have already occurred.[48] As the phenomenon is highly time-dependent, the input data must be updated regularly for the predictions to be accurate.[49] The phenomenon has most accurately predicted residential burglaries, but it has also been connected to other property-based crimes such as automobile theft.[50] While instructive, the fact that the studies are linked primarily with property crimes makes extrapolation to other categories of crime fairly limited.[51]

HunchLab similarly focuses on particular geographic areas and extrapolates the probability of crime occurring based on certain factors linked to those areas. However, HunchLab incorporates different theories and modeling techniques, such as risk terrain modeling.[52] Risk terrain modeling examines a variety of social, physical, and behavioral factors, each forming a layer with a certain probability of risk linked to a certain crime; these layers, in conjunction, create the probability of a certain crime happening in a specific area.[53] The most recent version of the program attempts to create a "unified prediction of crime" from a constellation of different theories, using data sources such as weather, socioeconomic indicators, historic crime levels, routine activity theory, and recurring events such as holidays or sporting events.[54] While PredPol relies solely on historical crime data and hotspot clustering,[55] HunchLab's algorithm relies on a broader array of information, i.e., variables other than the number of arrests in the area over time.[56]

48. Ferguson, *Predictive Policing*, *supra* note 2, at 277–78.

49. *See id*. at 312.

50. *See id*. at 317; *see also* Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 30 (2016) ("Predictive policing software, already in use by some police departments, focuses heavily on property crimes because its predictions about other crimes are not as accurate.").

51. *See* Ferguson, *Predictive Policing*, *supra* note 2, at 281.

52. *See* AZAVEA, HUNCHLAB: UNDER THE HOOD 5 (2015) [hereinafter HUNCHLAB], http://cdn.azavea.com/pdfs/hunchlab/HunchLab-Under-the-Hood.pdf [https://perma.cc/WY6U-TDRH].

53. Ferguson, *Predictive Policing*, *supra* note 2, at 281 ("[R]isk terrain modeling (RTM) offers a way of looking at criminality as less determined by previous events and more a function of a dynamic interaction between social, physical and behavioral factors that occurs at places.") (quoting Leslie W. Kennedy, Joel. M. Caplan & Eric Piza, *Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies*, 27 J. QUANT. CRIMINOL. 339, 342 (2011)).

54. HUNCHLAB, *supra* note 52, at 12.

55. *See* George Mohler, Martin B. Short, Sean Malinowski, Mark Johnson, George E. Tita, Andrea L. Bertozzi & P. Jeffrey Brantingham, *Randomized Controlled Field Trials of Predictive Policing*, J. AM. STAT. ASS'N 3, 4 (2015); *How PredPol Works*, PREDPOL, http://www.predpol.com/how-predpol-works/ [https://perma.cc/UJZ4-5H3Y].

56. *See* HUNCHLAB, *supra* note 52, at 10 ("We have spent the last few years determining how to incorporate multiple crime theories into one forecast. For example, we can incorporate concepts such as: temporal patterns (day of week, seasonality); weather; risk terrain modeling (locations of bars, bus stops, etc.); socioeconomic indicators; historic crime levels; and near-repeat patterns.");

HunchLab also determines what kind of data is the most useful for the crime it is predicting. For example, residential burglary is more likely to be deterred by law enforcement presence than is murder.[57] The predictions are thus more tailored than a broad assessment of "risk" alone.

The methodologies employed by HunchLab and PredPol create distinct concerns and have distinct Fourth Amendment analogues. PredPol's exclusive reliance on historical crime data, as opposed to HunchLab's panoply of different theories and data sources, creates a higher risk that the program will produce a self-perpetuating feedback loop of crime prediction.[58] Officers respond to a heightened probability of crime by increasing law enforcement presence in the area, which is likely to increase the volume of arrests, thus raising the crime rate for the area (and making the location more likely to be analyzed as high risk in the future). The determination of the area as high risk could be unduly influenced by the software's previous predictions, as opposed to a more current evaluation of a particular area's propensity for crime. The prediction is thus manufactured by the algorithm, rather than organically predictive, compromising its value. While HunchLab's more holistic (and thus seemingly more accurate) array of factors aims to counteract this issue,[59] the poor reliability of that array of factors could make its calculations just as flawed. Diversification is only an improvement if the source of the diversity is more accurate or reliable than the homogeneity it replaces.

Software that assigns individual threat scores is the newest iteration of the data-fueled trend in policing. A third program, Beware, derives an individualized risk assessment from data supplied by commercial data brokers and public records, which can include social media activity and health information.[60] Beware has

---

see also, *id*. at 12 ("Our belief is that the use of non-crime data sets as variables within a crime prediction system is important, because variables based solely upon crime data become skewed as predictions are used operationally. For instance, as crimes are prevented in mission areas due to police response, the only variables identifying areas as high risk are skewed in other systems. By including other data sets, our system is more robust against this issue.").

57. Maurice Chanmah & Mark Hansen, *Policing the Future*, THE MARSHALL PROJECT, Feb. 3, 2016, https://www.themarshallproject.org/2016/02/03/policing-the-future#.PwmMQID8e [https://perma.cc/975N-4EJB] (describing the St. Louis Police Department's use of HunchLab).

58. Ferguson, *Predictive Policing*, *supra* note 2, at 314–16; DAVID ROBINSON & LOGAN KOEPKE, UPTURN, STUCK IN A PATTERN: EARLY EVIDENCE ON "PREDICTIVE POLICING" AND CIVIL RIGHTS (2016), https://www.teamupturn.com/static/reports/2016/predictive-policing/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf [https://perma.cc/P92R-2SWE] ("[P]redictive systems that rely on historical crime data risk fueling a cycle of distorted enforcement.").

59. HUNCHLAB, *supra* note 52, at 12 (contrasting the company's methodology with systems that solely rely on historical crime data: "Our belief is that the use of non-crime data sets as variables within a crime prediction system is important, because variables based solely upon crime data become skewed as predictions are used operationally").

60. *See* Joh, *supra* note 50, at 24–25 (describing Beware); David Robinson, *Buyer Beware: A Hard Look At Police 'Threat Scores'*, EQUAL FUTURE, Jan. 14, 2016, https://www.equalfuture.us/2016/01/14/buyer-beware-police-threat-scores/ [https://perma.cc/SH7G-843T] ("According to promotional materials and public statements, these

released very little information about the methodology it employs, claiming its algorithms are protected as trade secrets. The company is ambiguous concerning the risks its assessments purport to predict; its "threat assessments," from least to most dangerous, simply report as green, yellow, or red, and are not precisely connected to past crimes.[61] The lack of guidance and transparency makes evaluating the program's accuracy difficult, thus rendering the use of threat scores more susceptible to error or abuse. Beware's heavy reliance on social media raises concerns of chilled speech,[62] as well as accuracy issues: these programs purport to provide police officers with relevant and reliable information, when that information is in fact stripped of its context. This was demonstrated to alarming effect at a city council briefing on the technology in Fresno, California. When a councilman asked "how a person gets to red," the police chief could not answer, because Intrado, the vendor, would not supply the information.[63] Running the councilman's own address through the system subsequently produced a yellow score, which the police department was also unable to account for.[64]

IV.
PREDICTIVE POLICING'S PITFALLS

No predictive policing software is self-executing. Regardless of methodology, an algorithm does not definitively declare that a crime will or will not happen, that a particular individual will or will not commit a crime, or how a police officer will act on that information. The method the algorithm uses to arrive at its determinations, the data it uses, and the way in which law enforcement officials are likely to act on that information are all crucial components in determining the impact of predictive policing on individual privacy and civil liberties.

Proponents of predictive policing software point to its empirical accuracy and the efficiency it offers to under-resourced police departments.[65] While limited positive results have been documented from risk terrain modeling, the reports are preliminary and largely inconclusive.[66] Moreover, most of the newer

---

threat scores may be based on everything from criminal histories to social media activity to health-related history.").

61. Robinson, *supra* note 60.

62. Jay Stanley, *Eight Problems With Police "Threat Scores"*, ACLU BLOG (Jan. 13, 2016, 10:30 AM), https://www.aclu.org/blog/free-future/eight-problems-police-threat-scores [https://perma.cc/X7KC-KJDA] (citing correspondence and internal Intrado documents obtained by the ACLU).

63. 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 [https://perma.cc/65ZU-LMHR].

64. Robinson, *supra* note 60.

65. Ferguson, *Predictive Policing*, *supra* note 2, at 269–70.

66. *See* Mohler, Short, Malinowski, Johnson, Tita, Bertozzi & Brantingham, *supra* note 55 (documenting preliminary positive results for the use of PredPol).

technologies, such as HunchLab and Beware, are too new for their effects to be fully evaluated or understood.[67] Even if the programs use accurate data and statistics, such accuracy does nothing to solve the problems that exist independent of empirical accuracy. Concerns that should be considered regarding the efficacy and legal impact of predictive policing algorithms can be categorized as follows: the empirical accuracy of input information; systemic bias embedded in the data and the structure of the algorithms; problems in applying new technology, such as automation bias; and lack of transparency, which precludes meaningful review or correction of these problems. Inaccuracy, discriminatory data and results, automation bias, and lack of transparency each limit the efficacy of predictive policing without clearly differentiating its likely impact from the use of current tools. These problems will dilute the reasonable suspicion standard if the technology is used without limits at the border.

A. Information Accuracy: Pyrite in Data Mining

While the empirical accuracy of predictive policing programs is not the sole problem with the technology, it remains a significant concern. An automated prediction is only as accurate as the information on which it is based. Data that is incorrect, haphazardly collected, or erroneously entered will lead to misguided determinations, and those determinations can only ever be as inherently effective, accurate, and useful as the subsequent actions they are used to justify.[68] Some prediction programs rely on commercial data brokers and data gleaned from social media, which risks producing acontextual and inaccurate results. Commercial data brokers—companies that aggregate data about consumers to sell for marketing and analytics purposes—operate with little accountability or oversight, and have been subject to considerable criticism for lack of transparency and low data quality standards.[69] Quality controls on existing policing data systems tend to be lacking, resulting in inaccuracies such as erroneous arrest reports.[70]

---

67. *See generally* Ferguson, *Predictive Policing*, *supra* note 2, at 314 ("Predictive algorithms are not magic boxes that divine future crime, but instead probability models of future events based on current environmental vulnerabilities. Creators of those algorithms understand that the limitations of the predictions rest in the limitations of the data and the conclusions drawn from the data.").

68. Stanley, *supra* note 62 ("There is nothing magical about taking a lot of data and creating a score; the algorithm by which that is done will do no more than reflect its creators' understanding of the world and how it works (at least if it is not based on machine learning—which I doubt this system is, and which in any case has other problems of its own).").

69. *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 16 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/WW6T-UJUJ] (noting the contracts between data brokers and their sources rarely address the accuracy of the provided information); Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105, 120 (2014) ("[P]redictive system performance is hindered on many levels, ranging from low quality data to flawed methodology to poor auditing and supervision. The first and most obvious barrier to predictive system performance is inaccurate input data.").

70. *See* Ferguson, *Big Data*, *supra* note 2, at 398.

Further, predictive policing algorithms rely on general statistical correlations. Even when mathematically sound, it is ethically problematic to entirely reduce an individual's agency to an amalgamation of demographic probabilities and fuzzy correlations.[71] For example, it would be empirically accurate to state that one in six black men has been incarcerated as of 2001, and that one in three will be incarcerated over the course of his life if current trends continue.[72] It would be immoral, unethical, and likely unconstitutional to incorporate that demographic probability into the prediction of an individual's likelihood to commit a crime in real time.

B. Beyond Empirical Accuracy

The biggest problem with substituting algorithmic techniques for existing methods is the perception of empirical neutrality and infallibility that data analytics tends to confer. In reality, an algorithm that relies on data produced by biased institutions and attitudes does nothing to inherently remove that institutional bias.[73] Machine-learning algorithms, for example, analyze a set of training data and design rules to apply to prospective data based on the relationship between various attributes in that initial set.[74] That means that any correlations between attributes like race and arrest rates can be recognized and replicated by the algorithm. This integrates discrimination into the software in a way that is subtle, unintentional, and difficult to correct, because it is often not the result of an active choice by the programmer.[75] Consider PredPol's sole reliance on historical crime data. If the majority of the arrests fueling the original predictions were racially motivated, this will produce higher law enforcement presence in the area. This presence will in turn produce more arrests, and the data from that encounter that is fed back to the algorithm will result in a prediction that the area is high risk.[76] When that data is used to assess the area as high crime, the prediction is no more neutral than the discriminatory stops that fueled it. Such a program is facially race-neutral, and attaches a degree of ostensible empiricism to the

71. *See* Robert Sprague, *Welcome to the Machine: Privacy and Workplace Implications of Predictive Analytics*, 21 RICH. J.L. & TECH. 1, 6–7 (2015) (discussing predictive algorithms and explaining the potential for researchers to overly rely on correlations).

72. *Criminal Justice Fact Sheet*, NAACP, http://www.naacp.org/pages/criminal-justice-fact-sheet [https://perma.cc/JJ2V-NSTG].

73. *See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

74. Jenna Burrell, *How The Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, BIG DATA & SOC'Y, Jan.–June 2016, at 5, http://bds.sagepub.com/content/spbds/3/1/2053951715622512.full.pdf/ [https://perma.cc/WA3V-28UX].

75. *See* Ferguson, *Big Data*, *supra* note 2, at 402 ("For example, the ACLU's recent national study on marijuana arrests demonstrates that African Americans are more likely to be arrested for marijuana than whites, despite equivalent usage rates. Thus, more data has been collected about minority marijuana possession, even though whites commit the crime at the same rate. If data are collected only about certain classes of people, then those people are more likely to become future targets of suspicion simply because of the initial selection bias.").

76. *See* ROBINSON & KOEPKE, *supra* note 58.

determination, without remotely correcting the underlying bias that has presumably been removed. The facial neutrality of the classifiers or the variables is irrelevant to the existence of bias in the algorithm: data analytics are designed to isolate correlated features and infer patterns that are not explicitly designated, with traits like race, gender, and socioeconomic status deductively encoded into the function of the algorithm.[77] Entrenching implicit bias through the choice of variables, or the particular criminological theories the algorithm relies on, poses similar concerns. Data can be skewed by the underreporting of crimes, or an enforcement focus on certain crimes or groups over others. Crime data does not reflect the rate at which crimes are committed; it measures the rate of crime that was caught and recorded.[78] The design of the algorithms can also be reflective of that analyst's worldview, and will produce results that are shaped by it.[79] Choice of variables and models can be mitigated, if not entirely cured, by increased transparency, such as through making the source code available. However, the institutional bias entrenched in the data itself, or perpetuated by user behavior, is much more difficult to isolate or correct, in addition to the problem that the reasoning behind the result of a machine-learning algorithm is often inexplicable.[80]

Ignoring the unintentional bias in machine learning algorithms poses a particularly insidious risk to disadvantaged groups by creating a pseudo-scientific justification for discriminatory treatment, inoculating those methods from criticism through supposed empiricism.[81] A general tenet of machine learning,

77. *See* Moritz Hardt, *How Big Data Is Unfair*, MEDIUM, Sept. 6, 2014, https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de#.asxzmuhfg [https://perma.cc/6UY3-W58N].

78. Ferguson, *Predictive Policing*, *supra* note 2, at 317; JONATHAN STRAY, THE CURIOUS JOURNALIST'S GUIDE TO DATA 8 (2016), https://www.gitbook.com/book/towcenter/curious-journalist-s-guide-to-data/details [https://perma.cc/H86B-NR8Y] ("Data is created. It is a record, a document, an artifact, dripping with meaning and circumstance . . . . Data production is an elaborate process involving humans, machines, ideas, and reality. It is social, physical, and specific to time and place."); ROBINSON & KOEPKE, *supra* note 58, at 5 ("Police statistics reflect enforcement, not just crime.").

79. Hardt, *supra* note 77.

80. Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter & Luciano Floridi, *The Ethics of Algorithms: Mapping The Debate*, BIG DATA & SOC'Y, July–Dec. 2016, at 1, 6 ("Algorithms can only be considered explainable to the degree that a human can articulate the trained model or rationale of a particular decision, for instance by explaining the (quantified) influence of particular inputs or attributes. Meaningful oversight and human intervention in algorithmic decision-making 'is impossible when the machine has an informational advantage over the operator . . . [or] when the machine cannot be controlled by a human in real-time due to its processing speed and the multitude of operational variables.'") (citations omitted), http://journals.sagepub.com/doi/pdf/10.1177/2053951716679679 [https://perma.cc/2Q5A-M7C6].

81. *See* Barocas & Selbst, *supra* note 73, at 674 ("Because the discrimination at issue is unintentional, even honest attempts to certify the absence of prejudice on the part of those involved in the data mining process may wrongly confer the imprimatur of impartiality on the resulting decisions. Furthermore, because the mechanism through which data mining may disadvantage protected classes is less obvious in cases of unintentional discrimination, the injustice may be harder to identify and address.").

and the large data sets those methods rely on, is that more is better— the larger the sample size, the more accurate the predictions, and the more the algorithm iterates, the more accurate and finely tuned it becomes.[82] This ignores the fact that when the accuracy of an algorithm is primarily contingent on the size of the data set, it will be less accurate for minority groups, for whom less data is generally available, and to whom rules based on majority-population features may not equally apply.[83]

In *Big Data's Discriminate Impact*, Solon Barocas and Andrew Selbst explore how both unintentional as well as deliberate choices by data mining analysts can produce discriminatory results.[84] Their discussion of unintentional disparate impact through the use of data mining in hiring and credit scoring mirrors the problems likely engrained in predictive policing algorithms. Like the determination that someone is a "good" employee or a "credit-worthy" customer, determining the likelihood that an individual will commit a crime is a subjective standard that must be reduced to highly specific attributes in order to be modeled in an algorithm. In addition to the risk that the algorithm will improperly eliciting sensitive or impermissible traits from the data, there is also a risk that policy objectives, such as a non-discriminatory prediction, will not (or cannot) be translated effectively into the way the algorithm is constructed. The difficulty of accurately translating broad language (such as "high smuggling") into the design of a location-based algorithm, for example, will enable substantial potential for unintended errors.[85]

C. Lost in Translation: Automation Bias

Automation bias stands for the proposition that individuals tend to rely on the judgments of automated decisions as superior to their own, even when they have

82. HUNCHLAB, *supra* note 52, at 16 ("HunchLab incorporates machine learning concepts to help the software 'think' like a crime analyst by imitating years of experience drawn from a police department's own data."); Mittelstadt, Allo, Taddeo, Wachter & Floridi, *supra* note 80, at 3 (defining machine learning and noting that "[t]he algorithm 'learns' by defining rules to determine how new inputs will be classified. The model can be taught to the algorithm via hand labelled inputs (supervised learning); in other cases the algorithm itself defines best-fit models to make sense of a set of inputs (unsupervised learning). In both cases, the algorithm defines decision-making rules to handle new inputs. Critically, the human operator does not need to understand the rationale of decision-making rules produced by the algorithm").

83. Hardt, *supra* note 77; *see also* Mittelstadt, Allo, Taddeo, Wachter & Floridi, *supra* note 80, at 7 ("Technical bias arises from technological constraints, errors or design decisions, which favour particular groups without an underlying driving value. Examples include when an alphabetical listing of airline companies leads to increase business for those earlier in the alphabet, or an error in the design of a random number generator that causes particular numbers to be favoured. Errors can similarly manifest in the datasets processed by algorithms. Flaws in the data are inadvertently adopted by the algorithm and hidden in outputs and models produced.") (citations omitted).

84. *See generally* Barocas & Selbst, *supra* note 73.

85. Citron, *supra* note 3, at 1262.

reason to believe the technology is flawed.[86] For example, predictive policing algorithms may be treated as inherently neutral and non-discriminatory by a court, while the information they provide nevertheless gives rise to discriminatory impact. Another example is a law enforcement officer's reliance on the technology in the field, despite mitigating circumstances that might have swayed his or her judgment otherwise. Substituting automated determinations for human decision-making can have unforeseeable consequences,[87] and algorithms are subject to the fallibility of the human being creating them, as well as the error of the human being interpreting their results.[88] One arguable antidote to automation bias is for human common sense to supplement and correct the insight of new technology. However, automation bias discourages such oversight,[89] rendering the corrective value of a semi-automated systems with human checks essentially meaningless.

D. Lack of Transparency

The value of transparency in government is both inherent and indirect. It is inherent, in that a democratic government assumes informed participation by the governed. It is indirect, in that it is a check on corruption or systemic flaws that would otherwise continue without public scrutiny. The inherent value of transparency is significant for predictive policing, such that police officers can understand the information they are receiving, and thus act on it appropriately, and judges can determine whether or not an officer's reliance on that information was reasonable. The indirect value of transparency is significant because of the problems outlined above that can be endemic to the use of algorithmic decision-making. Both kinds of transparency are essential for predictive policing to be used in an effective, legal, and ethical way that does not eviscerate the reasonable suspicion standard.[90] But transparency surrounding the use of predictive policing algorithms is widely lacking. Some companies, such as Intrado (the manufacturer of Beware), claim the right to shield the code powering their algorithms as trade secrets.[91] While those claims may be reasonable in some cases, if a police officer,

86. *Id*. at 1271–72 (citing Linda J. Skitka, Kathleen L. Mosier, Mark Burdick & Bonnie Rosenblatt, *Automation Bias and Errors: Are Crews Better Than Individuals?*, 10 INT'L J. AVIATION PSYCHOL. 85, 86 (2000)).

87. *Id*. (discussing the unpredictable pitfalls in automated solutions in legal systems).

88. *See* Kelly K. Koss, *Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in A Post-Wardlow World*, 90 CHI.-KENT L. REV. 301, 311 (2015).

89. *See* Citron, *supra* note 3, at 1271 (describing how human oversight as a check on automated administrative decisionmaking still resulted in widespread error due to automation bias).

90. *See* Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1521–23 (2013) (describing the increased implementation of data mining in government processes, the lack of transparency therein, and proposing corrections).

91. Jouvenal, *supra* note 63 ("Exactly how Beware calculates threat scores is something that its maker, Intrado, considers a trade secret, so it is unclear how much weight is given to a misdemeanor, felony or threatening comment on Facebook."); Elizabeth Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, N.Y.U. L. REV. ONLINE (forthcoming 2017) (manuscript at 19), https://ssrn.com/abstract=2924620 (noting that "[t]hough police departments

magistrate judge, or the public does not have access to how the predictions are made, there is no check on the legitimacy of the factors used. Nor is there a way to ascertain whether further decisions that relied on those determinations—such as a search, seizure, or arrest—were legally reached. There is no way for law enforcement, courts, legislatures, or the public to gauge the accuracy and value of the software without understanding how the methodology led to any purported success.

However, while transparency is the most effective check to the most egregious systemic problems, it is not the predictive policing panacea. Transparency can aid in preventing deliberate, or semi-deliberate discrimination, such as through the programmer's choice of variables, the methods of data collection, and departmental reliance on the programs, in a way that either permits or exacerbates automation bias. It would not correct the effects of the unintentional, institutional discrimination embedded in the data itself—arguably the most serious and difficult concern to counteract. Moreover, when the cause of a flawed result produced by a machine-learning algorithm is unknowable, transparency will do little to solve the underlying problem, apart from the value of revealing that the problem exists. Greater transparency is also unlikely to correct flaws in application, such as automation bias, and, to the extent that it leads to better programs, it can only aid in preventing arbitrary or discriminatory policing. If the use of these algorithms is transparent, but does not lead to the correction of encoded bias in the data or the use of poor-quality information, transparency is fairly hollow as an institutional principle. Transparency is primarily valuable for the solutions it can engender, not just the problems it reveals. It is necessary, but not sufficient, for predictive policing programs to be implemented in a transparent way to prevent a severe impact on the protection of individual rights at the border.

V.
APPLICATION OF PREDICTIVE POLICING AT THE BORDER

A. Predictive Policing and the Fourth Amendment

Prediction is already a part of Fourth Amendment jurisprudence, explicitly and implicitly.[92] A search warrant might rely on the prediction, based on probable cause, that contraband will be found at a certain location; pretrial detentions are

may rely increasingly on big data tools, they do not create them. The police are customers who contract with private vendors," and that both Predpol and Intrado guard their algorithms as trade secrets).

92. United States v. Cortez, 449 U.S. 411, 417 (1981) ("The process does not deal with hard certainties, but with probabilities. Long before the law of probabilities was articulated as such, practical people formulated certain common-sense conclusions about human behavior; jurors as factfinders are permitted to do the same—and so are law enforcement officers.").

predicated on the demonstrable likelihood, not certainty, of future acts.[93] Fourth Amendment analysis also frequently relies on anchoring broad probabilities to individual suspects, such as profiles,[94] and high crime areas,[95] or individualized predictions of possibly questionable reliability, such as reliance on informant tips.[96] Probabilistic and predictive techniques have also been considered or incorporated into other parts of the criminal justice system,[97] such as sentencing determinations.[98] Reasonable suspicion in particular is a flexible standard, based on probabilities, and is easy to square with predictive policing techniques. Previous scholarship has compared location-based predictive policing methodologies, like the hotspot mapping employed by PredPol or the risk terrain modeling employed by HunchLab, to courts' treatment of the high crime area designation in reasonable suspicion analysis.[99] Area-based programs can also be analogized to tip cases about locations in reasonable suspicion analysis.[100] Individual threat scores are most similar to courts' treatment of tips about individuals and the use of profiles in reasonable suspicion analysis.[101]

While concerning in other contexts, the use of these technologies is the most threatening to individual rights at the border, where the government prerogative to investigate is at its zenith, and Fourth Amendment protection for individual privacy is at its nadir. Stops at the border, by the simple fact of occurring at the border, do not require any individualized suspicion to be reasonable, and non-routine, highly invasive searches—such as strip searches, body cavity searches, or laptop searches—only need to be justified by an undefined degree of reasonable suspicion, rather than the standard probable cause.[102]

---

93. *See* Mark Noferi & Robert Koulish, *The Immigration Detention Risk Assessment*, 29 GEO. IMMIGR. L.J. 45, 56 (2014) ("pretrial detention is entirely forward-looking and predictive").

94. *See, e.g.*, Florida v. Royer, 460 U.S. 491, 493 n.2 (1983) (plurality opinion) ("The 'drug courier profile' is an abstract of characteristics found to be typical of persons transporting illegal drugs.").

95. Illinois v. Wardlow, 528 U.S. 119, 124 (2000).

96. Alabama v. White, 496 U.S. 325, 326–27 (1990); Illinois v. Gates, 462 U.S. 213, 225 (1983); Draper v. United States, 358 U.S. 307, 309 (1959).

97. *See generally* Laurence H. Tribe, *Trial by Mathematics: Precision and Ritual in the Legal Process*, 84 HARV. L. REV. 1329 (1971) (discussing the use of mathematical methods as a tool for decision-making in the actual conduct of a particular trial and in the design of the trial system as a whole).

98. *See generally* Sonja B. Starr, *Evidence-Based Sentencing and The Scientific Rationalization of Discrimination*, 66 STAN L. Rev. 803 (2014) (discussing the use of risk automation in sentencing and bail determinations).

99. *See generally* Ferguson, *Predictive Policing*, *supra* note 2; Ferguson, *Big Data*, *supra* note 2; Andrew Guthrie Ferguson, *Crime Mapping and the Fourth Amendment: Redrawing "High-Crime Areas"*, 63 Hastings L.J. 179 (2011) [hereinafter *Redrawing "High-Crime Areas"*]; 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) [hereinafter *High-Crime Area Question*].

100. Ferguson, *Predictive Policing*, *supra* note 2, at 308.

101. *Id*. at 288–92.

102. United States v. Ramsey, 431 U.S. 606, 611–13 (1977).

The question here is not whether predictive policing modeling that uses area-based predictions or threat scores would constitute an unreasonable search under the Fourth Amendment. While each has distinct constitutional implications, none rises to the level of an unreasonable search in and of itself.[103] The collected data used to generate the predictions must be exposed to human eyes to be considered a search for Fourth Amendment purposes.[104] Additionally, the third party doctrine—which holds that there is no reasonable expectation of privacy in information that has been shared with others[105]—would also likely undermine claims that this modeling constitutes an unreasonable search. Instead, the more relevant questions are (1) whether automated predictions can supply a level of reasonable suspicion constitutionally required to conduct an invasive, non-routine border search without further corroboration; and (2) what impact the use of automated predictions will have on individual rights when substituted for existing techniques in reasonable suspicion analysis, even when the predictions are supplemented by other facts.

It is highly unlikely that law enforcement officials will be instructed to rely solely on the technology, or that they would admit to having done so under oath: the promotional materials of these technologies all repeatedly declare that they are intended to enhance the trained judgment of law enforcement, not replace it.[106] Further, a judge would be unlikely to find that a single algorithmic prediction could create the basis for reasonable suspicion, as the totality of the circumstances test requires a range of factors, of which none is individually determinative.[107] The principle that no single factor can create reasonable suspicion is neither new nor unique to the use of predictive policing. Nevertheless, the end result may be primary reliance on the technology, due to automation bias.[108] The algorithm will

103. Joseph T. Thai, *Is Data Mining Ever A Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1734 (2006); Joh, *supra* note 50, at 34 ("In other words, surveillance that does not intrude upon recognized Fourth Amendment interests requires no prior justification by the police. The who, how, and why of police decisions to single out persons for attention is a matter of police discretion.").

104. *See Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 709 (2014) ("Kerr has argued that a computer's analysis of private information is irrelevant to the Fourth Amendment; a Fourth Amendment search should be found to occur only at the moment that a human interacts with private information.") (footnote omitted).

105. Smith v. Maryland, 442 U.S. 735, 743–45 (1979) (holding that the act of relaying numbers dialed to a phone company obviates the dialer's reasonable expectation of privacy).

106. *How PredPol Works*, *supra* note 55 ("PredPol does not replace the experience and intuition of our great officers, but is rather an invaluable added tool that allows our police force to use their patrol time more efficiently and helps stop crime before it happens.") (quoting Chief Mark Yokoyama); Chanmah & Hansen, *Policing the Future*, *supra* note 57 ("Dolly also recognized the fundamental limitation of the tool—it was 'telling you where to go,' he said. 'It's not telling you what to do.'") (quoting a St. Louis police officer regarding his use of HunchLab).

107. United States v. Rangel-Portillo, 586 F.3d 376, 380 (5th Cir. 2009) (citing United States v. Hernandez, 477 F.3d 210, 213 (5th Cir. 2007)).

108. Meg Leta Jones, *The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles*, 18 VAND. J. ENT. & TECH. L. 77, 91 (2015) (citing Kathleen L.

deliver a prediction, possibly inaccurate or skewed, that will nevertheless be likely to sway the officer's judgment. The result will be a dilution of the reasonable suspicion standard that is unlikely to be accounted for by courts, but which will have a significant impact on the protection of individual rights at the border.

This Article focuses on the impact of predictive policing on the reasonable suspicion standard because the non-routine, invasive searches that actually require reasonable suspicion at the border result in the most severe intrusions on individual privacy and rights. But the dilution of the reasonable suspicion standard is only part of the problem, due to the Fourth Amendment exceptions unique to the border context. When predictions are used to direct routine stops and searches at the border, their reasonableness is immaterial, as routine border stops do not require any degree of individualized suspicion.[109] The use of predictive policing at the border makes an even more forceful argument for the technology's critics, due to the Fourth Amendment's lesser protections for individuals in that context. Any concerns about the impact of predictive policing on Fourth Amendment rights—such as the perception of neutral empiricism,[110] high error rates,[111] and additional scrutiny of disadvantaged groups through the feedback loop effect[112]—become more urgent, as the border removes the mitigating protection of a reasonable suspicion requirement, and adds additional deference to the government. A stop prompted by a high threat score, or flight from a predicted high-crime area, must meet the standard of reasonable suspicion in Peoria; at the border, that same stop does not. And whatever degree of reasonable suspicion that justifies a limited stop and frisk in Peoria, would justify the police at the border to conduct an invasive search, such as an x-ray, or a search that destroys the defendant's property. Precisely which searches are routine and which are non-routine may not always be clear, as the Supreme Court has refused to define the parameters of potential transformation,[113] though a stop may become non-routine by virtue of degree of intrusion and scope. Either way, the use of the technology for routine stops and searches should also not be ignored.

B. Dilution of the Reasonable Suspicion Standard

Any attempt at analogizing new technology to previous Fourth Amendment doctrine should be undertaken with extreme caution. Seemingly transferable logic divorced of the basic assumptions that predicated it will produce enormously disparate results, with catastrophic ramifications for individual rights.[114]

Mosier, Linda J. Skitka, Susan Heers, & Mark Burdick, *Automation Bias: Decision Making and Performance in High-Tech Cockpits*, INT'L. J. AVIATION PSYCHOLOGY 47, 47 (1998)).

109. United States v. Ramsey, 431 U.S. 606, 616 (1977).

110. Ferguson, *Big Data*, *supra* note 2, at 401.

111. *Id*. at 398.

112. *Id*. at 403.

113. United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008).

114. *See generally* Riley v. California, 134 S. Ct. 2473, 2488–89 (2014). As Chief Justice Roberts wrote in the majority opinion in *Riley*, equating the modern cell phone with the typical

Reasonable suspicion, by virtue of its flexibility, is well-suited to incorporating new techniques, yet particularly susceptible to distortion by them. The ostensibly seamless comparison of predictive policing algorithms to old doctrine tempts the conclusion that they are not only comparable, but interchangeable. An algorithmic risk prediction seems like the automation of an officer weighing fact-specific circumstances, and determining the possibility of a crime occurring based on those facts. But an algorithm's determination of a high crime area or an individual's threat level is qualitatively and quantitatively distinct from an officer's judgment. An automated assessment is the product of a greater volume of information, which furthermore may be riddled with unknown errors, bias, or both. While an officer may make a mistake in judgment—a possibility the preexisting standard acknowledges—courts can understand and contextualize human error.[115] Courts are less likely to recognize or address the ways in which data mining works less accurately for minority groups, such that the risk predictions are less likely to be correct. They are equally unlikely to acknowledge broader flaws in the technology, such as the complications of automation bias, or how a risk assessment could confuse actual criminal propensity with tweeting about a card game, as occurred in the Fresno police department's test of Beware's individualized threat scores.[116] Ultimately, algorithmic predictions will be used with other facts that alone would be insufficient to satisfy the reasonable suspicion standard, such as a suspect's apparent race. That the predictions themselves are flawed will thus weaken the reasonable suspicion standard.

For example, a suspect's high threat score in a high-crime area might be analyzed to satisfy *Wardlow*'s standard for reasonable suspicion, even if the score was the product of discriminatory data, or automation bias affected the officer's judgment. The automated prediction of an area as "high crime" (or more likely "high smuggling," in the border context)[117] might be the product of a feedback effect, and yet still suffice for a finding of reasonable suspicion in conjunction with one or two other factors, such as the apparent Mexican ethnicity of the subject. The factors corroborating the predictions would not satisfy the standard without other supporting evidence (such as race of the suspect alone,[118] or the

closed container "is like saying a ride on horseback is materially indistinguishable from a flight to the moon . . . . A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom." *Id.*

115. United States v. Cortez, 449 U.S. 411, 417 (1981).

116. Jouvenal, *supra* note 63.

117. United States v. Salazar, 628 F. App'x 265, 266 (5th Cir. 2015) (citing United States v. Jacquinot, 258 F.3d 423, 427 (5th Cir. 2001) ("Additionally, the Border Patrol Agents were aware that Highway 131 was a known smuggling route that circumvented permanent immigration checkpoints. Although that alone is insufficient to justify a stop, the 'road's reputation as a smuggling route *adds* to the reasonableness of the agents' suspicion.'") (citations omitted).

118. United States v. Brignoni-Ponce, 422 U.S. 873, 886–87 (1975) ("The likelihood that any given person of Mexican ancestry is an alien is high enough to make Mexican appearance a relevant factor, but standing alone it does not justify stopping all Mexican-Americans to ask if they are aliens.").

history of the area alone[119]), while the predictions could themselves be incorrect or discriminatory. And yet the result would be a finding of reasonable suspicion where, due to a flawed prediction bolstering the validity of otherwise insufficient factors, reasonable suspicion does not exist. Courts have previously "rounded up" an aggregation of otherwise insufficient factors, such as the area's reputation as a known smuggling route,[120] the proximity of a vehicle to the border,[121] or that two cars are traveling together,[122] and have little reason not to do so for the use of automated predictions.

The seamless transfer of old doctrine to new technology is particularly dubious for the reasonable suspicion standard, a body of law based on human observations that is now increasingly confronted with the use of big data in similar circumstances.[123] The sheer volume and accessibility of information available about an individual at any given time makes reasonable suspicion an easier threshold to reach, weakening the Fourth Amendment's protection against invasions of privacy and civil liberties. The dilution of the reasonable suspicion standard is a fairly logical consequence of a wider availability of information about individuals. The exponential increase in information about a given suspect, and the mobility and accessibility of that information to officers in the field, necessarily changes the judicial calculus upon which the reasonable suspicion doctrine is based.[124] The standard is both weakened and distorted when the information is incorrect, out of date, or structurally suspect due to entrenched bias in the data and the structure of the algorithm. Moreover, the increased volume of information available is equally impactful if it is correct, as the Supreme Court has held in prior cases that even innocent facts, if they lead to a logical conclusion of likely criminal activity in aggregate, can suffice to establish reasonable suspicion.[125] Though an officer cannot "rely solely on generalizations that, if accepted, would cast suspicion on large segments of the law-abiding population,"[126] this does not contradict the aggregation principle, and could also be overruled in the case of threat scores, where determinations are categorically individualized. Predictive policing technology lowers the reasonable suspicion

119. *Salazar*, 628 F. App'x at 266.

120. *Id*.

121. United States v. Zapata-Ibarra, 212 F.3d 877, 881 (5th Cir. 2000).

122. *Salazar*, 628 F. App'x at 266 (citing United States v. George, 567 F.2d 643, 645 (5th Cir. 1978); United States v. Munoz-Martinez, 435 F. App'x 333, 335 (5th Cir. 2011) (citing *Jacquinot*, 258 F.3d at 427–28 ("A collection of factors that usually constitute innocent behavior may add up to reasonable suspicion in the mind of an experienced officer.")).

123. Ferguson, *Big Data*, *supra* note 2, at 351 ("[T]he growth of 'big data' has the potential to change the reasonable suspicion calculus because more personal or predictive information about a suspect will make it easier for police to justify stopping a suspect.").

124. *Id*.

125. *See* United States v. Arvizu, 534 U.S. 266, 277 (2002) (holding that the totality of circumstances test permits a valid determination of reasonable suspicion even when based on individually innocent or insufficient facts).

126. United States v. Cotterman, 709 F.3d 952, 994 (9th Cir. 2013) (quoting United States v. Manzo-Jurado, 457 F.3d 928, 935 (9th Cir. 2006)).

threshold, and at the border, that lowered threshold allows more severe intrusions than anywhere else.

The following section contains two parts. First, it will compare the reasonable suspicion analysis of area-based predictive policing technology to reasonable suspicion analysis that considers the characteristics of a certain area of the border; then, it will compare the analysis of an officer's use of threat scores to analysis of the use of tips about individuals or profiling. These comparisons are intended to demonstrate the similarity of predictive policing to existing doctrine, such that the flaws in the technology are likely to be ignored by courts, as well as the impact on individual rights that will result from ignoring those flaws. These two comparison sections will be followed by two hypothetical fact patterns, one involving an area-based predictive program, another with an automated risk assessment. These hypotheticals illustrate the impact of the unlimited use of predictive policing technology on individual rights under Fourth Amendment border doctrine, and demonstrate the resulting heightened governmental prerogative to intrude upon those rights.

C. High Crime Areas and Area-Based Predictive Policing at the Border

In terms of analogizing area-based predictive policing programs to Fourth Amendment doctrine, most efforts have focused on courts' treatment of the "high crime area" in finding reasonable suspicion for a stop.[127] In *Illinois v. Wardlow*, the Supreme Court held that a suspect's flight from a police officer, in an area the police officer determines to be high crime, establishes reasonable suspicion for a stop and frisk.[128] The Supreme Court has not defined what constitutes a high crime area, nor have subsequent cases managed to sharpen its initial determination into workable criteria for comparison, though numerous factors have been considered.[129] In the border context, an area used "predominantly for illegal purposes . . . is strong support for a finding of reasonable suspicion,"[130] but "a location or route frequented by illegal immigrants, but also by many legal residents, is not significantly probative to an assessment of reasonable suspicion."[131] That analysis is generally similar to that of high crime areas in other contexts; an officer's determination that the character and history of a location, in combination with other factors, increases the likelihood that the individual is committing or likely to commit a particular crime, weighs towards a finding of

127. *See generally* Ferguson, *Redrawing "High-Crime Areas"*, *supra* note 99; Ferguson & Bernache, *supra* note 99; Koss, *supra* note 88.

128. Illinois v. Wardlow, 528 U.S. 119, 124 (2000).

129. Ferguson, *Redrawing "High-Crime Areas"*, *supra* note 99, at n.21 (quoting Adam Carlis, *The lllegality of Vertical Patrols*, 109 COLUM. L. REV. 2002, 2010 (2009)).

130. United States v. Manzo-Jurado, 457 F.3d 928 (9th Cir. 2006) (citing *Arvizu*, 534 U.S. at 269).

131. *Id.*

reasonable suspicion.[132] At the border, those considerations have included the use of the route, either for smuggling or for recreation, its proximity to the border, typical traffic patterns, or "information about recent illegal border crossings in the area."[133] The term "high crime area" itself has been used in border-context reasonable suspicion cases, and like the high crime area cases in other contexts, mere presence in an area known for a high degree of smuggling is insufficiently probative.[134]

The factors that courts have cited in high crime area analysis are analogous to the factors that would be used to calculate risk of crime in an area-based predictive policing program. The probability that a certain area of the border is more likely to be crossed, or a traditional smuggling route, is impacted by geography, time, and weather, all factors that can be used in risk terrain modeling.[135] The past use of the route for illegal activity is directly transferrable to PredPol's reliance on historical crime data.[136] Following that logic, the broader array of factors upon which risk-terrain modeling relies, such as weather, time of day, season, or holiday should also be transferrable. However, the list of possible factors is endless and often self-contradictory, rendering accurate, reliable, and standardized variables difficult to come by.[137] Further, when an area is determined to be high crime, only one additional factor is required for a finding of reasonable suspicion, such as flight from an officer.[138] The flexibility of the standard is problematic because it allows the reasonable suspicion analysis to tip further in the government's favor. But at the border, courts already afford the government more leeway than anywhere else.[139] The willingness of courts to accept a determination of high crime based on an extensive, malleable, and often contradictory set of facts indicates the likelihood that an automated determination of the high crime area

132. *Arvizu*, 534 U.S. at 277 ("The likelihood that respondent and his family were on a picnic outing was diminished by the fact that the minivan had turned away from the known recreational areas accessible to the east on Rucker Canyon Road. Corroborating this inference was the fact that recreational areas farther to the north would have been easier to reach by taking 191, as opposed to the 40-to-50-mile trip on unpaved and primitive roads.").

133. United States v. Brignoni-Ponce, 422 U.S. 873, 884–85 (1975).

134. United States v. Rangel-Portillo, 586 F.3d 376, 381 n.3 (5th Cir. 2009) ("Absent some other contributing factor, merely driving in an area 'notorious for alien smuggling,' alone, does not constitute reasonable suspicion.").

135. *See supra* note 56 and accompanying text.

136. *See* United States v. Garza, 727 F.3d 436, 440 (5th Cir. 2013) (noting that the court has previously that held travel along routes frequented by border traffic "weighs in favor of reasonable suspicion").

137. *See* United States v. Zapata-Ibarra, 223 F.3d 281, 282 (5th Cir. 2000) (Wiener, J., dissenting) (criticizing the "emasculation" of the Fourth Amendment at the border due in part to an endless list of factors that have been held to be persuasive, often in contradictory cases).

138. *Id*. at 442 ("Unprovoked flight, as well as nervous, erratic behavior, are factors which support a finding of reasonable suspicion, especially in a border case.") (citations omitted).

139. *See* United States v. Flores-Montano, 541 U.S. 149, 153 (2004) ("It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."); United States v. Ramsey, 431 U.S. 606, 616 (1977) ("[S]earches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border.").

will be accepted for reasonable suspicion analysis, regardless of the fact that the prediction may be mistaken or skewed.[140]

The confluence of the "thumb on the scale" that a finding of a high crime area provides in establishing reasonable suspicion; and the heightened government prerogative to investigate due to the diminished Fourth Amendment protections at the border, make an automated prediction of what "high crime" means particularly concerning. Reasonable suspicion at the border permits a far greater degree of intrusion than it does in other contexts, where reasonable suspicion only permits the officer to stop, question, and possibly frisk the subject, depending on the suspected activity. At the border, reasonable suspicion can justify non-routine searches like x-rays, strip searches, and searches of body cavities, provided that suspicion is related to a criminal activity that is tied to the border, particularly contraband smuggling, alien smuggling, or other immigration violations.[141] The border context alone permits the degree of intrusion that the high crime area is invoked to justify.

D. Profiling, Tips About Individuals, and Individual Threat Scores

There are two strains of Fourth Amendment jurisprudence that bear heavily on the constitutionality of threat scores. The first involves tips about a particular suspect, while the second concerns the matching of a suspect's conduct or characteristics to an established profile.[142] As with area-based predictive algorithms and high-crime areas, the border context significantly changes the analysis, and analogizing old doctrines to new solutions must be done with nuanced attention to the original logic underlying those theories. A broad profile which, if judicially sanctioned as the basis for reasonable suspicion, would cast suspicion on broad categories of innocent people, is insufficient.[143] Further, while an individual's adherence to a generalized profile may be considered an element of reasonable suspicion, similarity to a profile must still be linked to specific observations about the suspect, and his or her individualized and particularized likelihood to commit a crime.[144] Profiles that have been previously sanctioned by the courts in the border context include profiles of drug smugglers[145] and "alien

140. *See* Illinois v. Wardlow, 528 U.S. 119, 124–25 (2000) ("[C]ourts do not have available empirical studies dealing with inferences drawn from suspicious behavior, and we cannot reasonably demand scientific certainty from judges or law enforcement officers where none exists.").

141. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . .") (citations omitted).

142. In the border context, the profile would usually be that of an illegal alien, or of a smuggler of either aliens or contraband.

143. *See* United States v. Manzo-Jurado, 457 F.3d 928, 935 (9th Cir. 2006) ("[A]n officer cannot rely solely on generalizations that, if accepted, would cast suspicion on large segments of the lawabiding population.").

144. *See id*.

145. *Id*. at 935; United States v. Sokolow, 490 U.S. 1, 10 (1989).

smugglers."[146] Indications of past crimes, or an officer's assessment of the likelihood of general criminal propensity or associations, are also insufficient as uncorroborated criteria for a stop.[147]

Similar to their treatment of profiles, courts have allowed tips about individuals from informants and anonymous sources to justify reasonable suspicion when the tip is one component of the totality of the circumstances.[148] Generally, the reasonableness of an officer's reliance on a tip is gauged by the quality of the information and the quality of the source, where the strength of one can outweigh the deficiency of the other.[149] A court will analyze a tip's veracity (the extent to which the prediction was ultimately correct); the tipster's reliability (the extent to which the source is trusted, ranging from anonymous sources to established informants); and the tipster's basis of knowledge (the quality of the tipster's source).[150] In a sliding scale, tips from anonymous sources or untrustworthy informants require a greater degree of independent corroboration by the officer to constitute reasonable suspicion, whereas less corroboration is required for known or previously reliable informants.[151]

Tips and profiles are each instructive in considering a court's approach to the use of threat scores in reasonable suspicion analysis. Profiles establish a baseline probability that, considering a certain set of characteristics that have repeatedly been linked to perpetrators of certain types of crimes, there is some basis for the inference that an individual with that set of characteristics might be more likely to commit a crime of that type than someone who does not possess those characteristics. In both basic profiling, and when using a risk-assessment algorithm, similarity to a profile is necessary, but not sufficient to establish reasonable suspicion of wrongdoing. The observations must be anchored to the particular individual, the particular set of circumstances, and a particular crime.[152] A tip about an individual is also comparable to an individualized threat score, in that it indicates the likelihood of an individual committing a crime in the future, and must also be corroborated.

---

146. United States v. Arvizu, 534 U.S. 266, 269, 277 (2002) (describing the facts that led to the officer's determination that the defendant met a smuggling profile, including the route taken and the perception that the defendant's children were acting in a mechanical way).

147. *See Sokolow*, 490 U.S. at 12 (Marshall, J., dissenting) ("It is not enough to suspect that an individual has committed crimes in the past, harbors unconsummated criminal designs, or has the propensity to commit crimes. On the contrary, before detaining an individual, law enforcement officers must reasonably suspect that he is engaged in, or poised to commit, a criminal act *at that moment*.").

148. *See* Illinois v. Gates, 462 U.S. 213, 231–32 (1983).

149. *See id*.

150. *See id*.; Alabama v. White, 496 U.S. 325, 328–29 (1990).

151. *White*, 496 U.S. at 328–29.

152. United States v. Manzo-Jurado, 457 F.3d 928, 939 (9th Cir. 2006) ("Although an officer, to form a reasonable suspicion of criminality, may rely in part on factors composing a broad profile, he must also observe additional information that winnows the broad profile into an objective and particularized suspicion of the person to be stopped.").

A court could analyze threat scores in one of two contradictory ways. A judge might determine that a risk assessment is either inherently generalized, as it is based on broad correlations, or inherently individualized, as the profile is personally linked to the suspect. It is arguable that an individual threat score, by definition, is individualized and particularized, as it assembles a vast array of probabilities in a combination that only the particular individual may have. But algorithms are based on statistical generalities, which are inherently broad and un-individualized; declaring that demographic probabilities are determinative reduces Fourth Amendment analysis to pseudoscience.[153] Ultimately, considering the extent to which courts have approved of the use of profiles, it is highly likely that individualized threat scores would be considered a permissible factor for reasonable suspicion analysis.

E. Area-Based Hypothetical

Imagine that Customs and Border Protection employs an area-based predictive policing software, which relies on a compendium of different criminological theories and modeling methods, including risk terrain modeling and hotspot mapping. The program has indicated that a certain area has a significantly heightened probability of drug smuggling that day, though the date, time, and other surrounding circumstances, such as the weather, and the typical use of the area, appear innocuous to patrolling Officer Bob, an experienced officer.[154] The vehicle is unremarkable, neither overly flashy nor overly shabby, and is not a particular make and model previously tied to smuggling; the car is ten miles away from the border.[155] Officer Joe sees Maria, who is Latina, and driving at the speed limit, and did a double take when she saw the officer, then nodded in his direction. It is 8:30 AM on a Monday and her clothes are oddly dirty and rumpled. Deciding that her demeanor in an area considered "high-smuggling" seemed suspicious, he gestures to her from a few yards away and asks her to stop.

---

153. *See* Hannah Wallach, *Big Data, Machine Learning, and the Social Sciences: Fairness, Accountability, and Transparency*, MEDIUM, Dec. 19, 2014, https://medium.com/@hannawallach/big-data-machine-learning-and-the-social-sciences-927a8e20460d#.4721nzoi2 [https://perma.cc/E27C-B8WD] (discussing granularity in data mining); *see also* Andrej Zwitter, *Big Data Ethics*, BIG DATA & SOC'Y, July–Dec. 2014, at 4, http://bds.sagepub.com/content/spbds/1/2/2053951714559253.full.pdf [https://perma.cc/NS84-BGEX] (discussing the ethical implications of big data revelations of criminal propensity).

154. *See, e.g.*, United States v. Olivares-Pacheco, 633 F.3d 399, 405 (5th Cir. 2011) (describing evidence proffered by the government that the related stop occurred at "Monday at 10:30 A.M." as "about the most innocuous conceivable hour").

155. *See id*. at 405 ("[T]he vehicle was unremarkable in all respects—it was neither 'too clean' nor 'too dirty,' neither over- nor under-loaded, neither brand new nor ancient, nor did the agents articulate that this was a brand or style known for alien smuggling, etc."); United States v. Rivera-Gonzalez, 413 F. App'x 736, 739 (5th Cir. 2011) ("The extreme cleanliness of a vehicle is significant in a rural area where such clean vehicles are unusual."); United States v. Garcia, 732 F.2d 1221, 1224 (5th Cir. 1984) ("The evidence also adequately supports the district court's unchallenged finding that the agents knew that campers are used frequently for transporting illegal aliens.").

This scenario could provide reasonable suspicion for a non-routine search, based on the prediction that the area was high-smuggling, Maria's apparent ethnicity, the proximity to the border, and behavior and appearance within the range of previously accepted factors. Outside of the border context, this is unlikely to satisfy reasonable suspicion; most of the plus factors here (proximity to the border; mildly evasive behavior; and an explicit consideration of Maria's ethnicity) are unique to the border context. But while these facts would likely suffice for reasonable suspicion at the border, the officer's judgment to stop Maria would not even have to meet that standard unless the ensuing stop or search was non-routine. Routine stops do not require any element of reasonable suspicion, so whether or not the predictions satisfied the standard would be irrelevant.[156] If the stop or search crossed the undefined threshold[157] and became non-routine, some degree of individualized suspicion would be warranted. In an identical scenario occurring outside the border context, this set of facts would unlikely satisfy reasonable suspicion, and if it did, the police would only be entitled to a stop or brief frisk, as opposed to an invasive search. The key risk here is that the automated assessment will make the officer more likely to stop Maria, when that judgment will either be required only to meet a standard of reasonable suspicion (if a non-routine search or seizure ensues), or no standard at all (if the stop or search is routine).

The concern that the use of predictive policing will increase discriminatory policing of minorities[158] is far more serious at the border, where routine stops will not be subject to the degree of judicial scrutiny that the same stops outside of the border context must satisfy. The list of factors comprising the standard for what constitutes a reasonable search or seizure at the border is already highly variable and can explicitly include the race of the suspect. If one of those factors is an automated prediction that courts will perceive as more neutral and more legitimately reliable than it is, the slim protections for individual rights currently in place at the border will be further diminished. In *Illinois v. Wardlow*, the Court held that a suspect's flight from a high-risk area creates reasonable suspicion; at the border, reasonable suspicion is sufficient justification for a cavity search.[159] The threshold determination in the analysis of whether the area is "high crime" creates a feedback effect where the prediction is bolstered by a combination of

156. *See* United States v. Ramsey, 431 U.S. 606, 616 (1977).

157. *See supra* note 23 and accompanying text.

158. *See* Melissa Hamilton, *Back to the Future: The Influence of Criminal History on Risk Assessments*, 20 BERKELEY J. CRIM. L. 75, 132 (2015) (discussing the use of proxies like criminal history for race in automated risk assessments); Alexander H. Kipperman, *Frisky Business: Mitigating Predictive Crime Software's Facilitation of Unlawful Stop and Frisks*, 24 TEMP. POL. & CIV. RTS. L. REV. 215, 236 (2014) (noting that statistical evidence showed that "the geographically large" High Crime Area designations in New York City "enable[d] and perpetuate[d] a trend of unconstitutional stops based on race"); Ferguson, *Predictive Policing*, *supra* note 2, at 301.

159. *See* Illinois v. Wardlow, 528 U.S. 119, 124 (2000); United States v. Garza, 727 F.3d 436, 442 (5th Cir. 2013) ("Unprovoked flight, as well as nervous, erratic behavior, are factors which support a finding of reasonable suspicion, especially in a border case.") (citations omitted).

factors that otherwise would not provide reasonable suspicion for a stop, search, or seizure.

F. Profiling Hypothetical

Consider the same hypothetical from above, with some minor adjustments. Imagine that Customs and Border Protection employs an individualized risk-assessment program, which relies on various data sources. Officer Bob, an experienced officer, sees José, who appears Latino, and driving alone.[160] The area, date, time of day, and weather are unremarkable,[161] and the road is not a known smuggling route, though it is just ten miles from the border.[162] The vehicle is unremarkable, neither overly flashy nor overly shabby, and is not a particular make and model previously tied to smuggling.[163] José is driving at the speed limit, and did a double-take when he saw the officer, then nodded in his direction. Deciding that José's demeanor seems suspicious, Bob gestures to him from a few yards away and asks him to stop. He then runs José's threat score, which comes back as red, indicating that the probability of his being a drug smuggler as extremely high.

Just as with the area-based prediction hypothetical, the automated prediction will likely lend enough credence to an otherwise insufficient set of factors to create reasonable suspicion. In the border context, the combination of factors will not be subject to reasonable suspicion analysis, provided the ensuing stop is routine. And if the encounter does result in an invasive search requiring reasonable suspicion, the "heightened prerogative of the sovereign" will likely tilt the analysis in favor of the government. The explicit sanction of ethnicity as a consideration in profiling further exacerbates the risk of broad profiles being used, whether deliberately or as a vehicle of implicit bias, to target minorities.[164] That race can serve as an explicit consideration for reasonable suspicion at the border is particularly

160. *See, e.g.*, United States v. Olivares-Pacheco, 633 F.3d 399, 408 (5th Cir. 2011) ("A lone Hispanic male was driving, and the vehicle was registered in someone else's name, both facts that are common among drug smugglers.") (citing United States v. Samaguey, 180 F.3d 195 (5th Cir. 1991)).

161. *See supra* note 155 and accompanying text.

162. *See* United States v. Montero-Camargo, 208 F.3d 1122, 1139 (9th Cir. 2000) ("The fact that the cars had Mexicali license plates may also provide some additional weight, given all the other circumstances. While having Mexican plates is ordinarily of no significance, where the criminal act suspected involves border-crossing, the presence of foreign license plates may be afforded some weight in determining whether a stop is reasonable.").

163. *See supra* note 155 and accompanying text.

164. Hamilton, *supra* note 158, at 130–32; Bernard E. Harcourt, *Risk as a Proxy for Race*, 27 FED. SENT'G REP. 237, 237 (2015) ("[W]e should resist the political temptation to embrace the progressive argument for risk-prediction instruments because their use will unquestionably aggravate the already intolerable racial imbalance in our prison populations.").

concerning for the use of automated profiles, when there is a high risk of error[165] and machine-learning methods can be less accurate for minority groups.[166]

The problems with both profiling and area based predictions in the border context are the explicit sanction of race as a consideration, the government's heightened prerogative to investigate at the border, and the fact that reasonable suspicion is not required for a routine stop or search. However the technology might skew its predictions, whether due to implicit bias, poor implementation, or simple error, those errors would not even be analyzed for reasonableness when used for the routine stop or search, in light of judicial deference to the government. At the very least, non-routine searches require some degree of individualized suspicion, which area-based predictions and threat scores would be required to meet. But individualized suspicion must corroborate other factors, which include a long list of contradictory considerations. The result is a severe extension of the power to intrude compared to the degree of justification required.

These two hypotheticals underscore the laxity of the reasonable suspicion standard at the border, and, given the malleability of the standard, the extent to which flawed predictions are likely to weaken it further. It is fairly unlikely that a law enforcement official would admit to sole reliance on such technology as a source for reasonable suspicion, both because it seems unreasonable after the fact, and because it is highly likely that he or she would have received instructions that the technology is only meant to supplement his or her professional judgment. Moreover, the reasonable suspicion doctrine does not allow for sole reliance on any one factor.[167] It is highly unlikely for a situation to arise in which there are truly no other indicators that could confer reasonable suspicion—or in which the officer would admit that there were no other factors—given the long list of possible factors available.[168] The greater concern is when reliance on the technology at the behest of other indicators is not a deliberate decision, but the result is nevertheless that the technological assessment was the determinative factor. Predictive policing technology, despite considerable flaws that affect the quality and reliability of their predictions, will provide an additional thumb on the reasonable suspicion scale, in addition to that which is already provided by the border context's lower standard. This is far from even-handed justice.

These two hypotheticals also illustrate why predictive policing poses a uniquely severe threat to individual privacy and civil liberties at the border. The

165. *See Olivares-Pacheco*, 633 F.3d at 408 ("A lone Hispanic male was driving, and the vehicle was registered in someone else's name, both facts that are common among drug smugglers.").

166. Hardt, *supra* note 77, at 4–5 ("The negative effects of sample size disparities are greatly exacerbated by the existence of cultural differences . . . . The lesson is that statistical patterns that apply to the majority might be invalid within a minority group. In fact, a variable that's positively correlated with the target in the general population, might be *negatively* correlated with the target in a minority group.").

167. United States v. Rangel-Portillo, 586 F.3d 376, 379–80 (5th Cir. 2009) (citing United States v. Hernandez, 477 F.3d 210, 213 (5th Cir. 2007)).

168. *See supra* note 30 and accompanying text.

Supreme Court held in *Whren v. United States* that the subjective motive of a police officer has no bearing on the reasonableness of a stop, even when that motive includes race.[169] In contrast, consideration of a person's race or national origin is an accepted indication of reasonable suspicion under *Brignoni-Ponce*;[170] it may not be the only factor upon which the analysis relies, but it may be a directly articulated factor the officer takes into consideration. The use of race as a factor or proxy in an algorithm might be legitimately criticized (or even illegal) in other contexts, such as an automated assessment of an applicant's suitability for credit. That a suspect's apparent race is a legal consideration at the border means that critiques of race proxies in a predictive policing algorithm used at the border may be less persuasive. Further, the reasonable suspicion that an automated prediction could confer beyond the border context—whether in comparison to a tip about an individual, an individual's similarity to a profile, or determining an area as high crime—could only justify a stop, and if relevant to the content of the suspicion, a limited search.[171] In contrast, such a prediction at the border, in conjunction with an endless laundry list of mutually contradictory factors, can justify an x-ray, prolonged detention, or a cavity search.

VI.
PRELIMINARY RECOMMENDATIONS

The Fourth Amendment is an ill-adapted bulwark against predictive policing programs, which lower the threshold of reasonable suspicion without qualifying as a search or seizure in and of themselves. Existing statutes and regulations promulgating Customs and Border Protection authority to search and seize are equally insufficient to guard against the threat these programs pose. If the Fourth Amendment provides insufficient protection, the options are to adjust the standard, ban the use of predictive policing in the border context, or to rigorously limit its use.

The same set of facts can also prompt a contradictory conclusion. It can be argued that as the risk of external threats at the border mandates a heightened governmental prerogative to investigate those threats, the use of any legally justifiable tools should be permitted, or even encouraged, for the sake of national security. In a vacuum, balancing the individual rights of the citizenry against the security of the nation as a whole, that argument has some validity. But it fails to take into account the discriminatory results that will ensue from unlimited use of the technology in this particular case. For some, the goal of collective safety merits a unilateral sacrifice of some degree of individual rights in this particular context.

---

169. Whren v. United States, 517 U.S. 806, 812 (1996).

170. United States v. Brignoni-Ponce, 422 U.S. 873, 886–87 (1975) ("The likelihood that any given person of Mexican ancestry is an alien is high enough to make Mexican appearance a relevant factor, but standing alone it does not justify stopping all Mexican-Americans to ask if they are aliens.").

171. *See* Terry v. Ohio, 392 U.S. 1, 30 (1968).

But that calculus must change if the sacrifice is not collective, but instead confined to minority groups, or becomes fundamentally arbitrary by virtue of an unacceptable degree of error. Predictive policing technology, at this stage of its development, is far closer to the latter.

In his comprehensive article *Big Data And Reasonable Suspicion*, Andrew Guthrie Ferguson explores the idea of a heightened reasonable suspicion standard for the use of big data, noting that may not be the most realistic approach.[172] In the border context, proposing a heightened standard for the use of big data is all the more unrealistic, considering the long-standing deference to the prerogative of the government to investigate threats at the border.[173] Moreover, reasonable suspicion is required only for invasive searches. A heightened reasonable suspicion standard would not address how the use of the technology would affect Fourth Amendment protections against routine stops.

That leaves the question of whether the use of predictive policing at the border should be limited or banned outright. That is both a normative question and a pragmatic one: one has to consider both the likely implications of this technology on individual rights, and how that effect should be mitigated, against what legislative protections are possible outside of an idealized moral vacuum, given public perception and political will. A blanket ban on the use of predictive policing technology at the border would be politically untenable. Even if that were not the case, such a prohibition would needlessly halt potentially positive uses of the technology. Statutory standards that mitigate the potential harms of predictive policing without banning it outright could allow law enforcement officers to harness the benefits of increased efficiency and accuracy. However, it is impossible to ignore that the most potentially invidious problems with predictive policing may be the most difficult to correct. No amount of testing or data quality standards can override human fallibility or automation bias, or magically strip a dataset of the institutional discrimination that produced it. Nevertheless, checks on concerns like data quality, empirical accuracy, training, and lack of transparency would be a promising beginning. The following section proposes some basic safeguards that could reduce the potential of predictive policing to dilute the reasonable suspicion standard past recognition.

A. Mandating Data Quality and Accuracy

The first step to ensuring that predictive policing can be used in an accurate, legal, and ethical way is to mandate rigorous testing and data quality standards to avoid errors in application to both majority and minority groups. Concerning as rampant errors and low data quality standards are in a consumer context (as with

172. Ferguson, *Big Data*, *supra* note 2, at 405.

173. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.").

automated credit scoring or hiring searches), they can produce even more egregious harms in the criminal justice context.[174] If your credit score is based on faulty data, you could be denied a loan. If your threat score results from erroneous correlations, you could be subject to a humiliating body cavity search.[175] The stakes are radically higher. In examining possible solutions to the due process problems posed by automated decision-making in administrative law,[176] Professors Danielle Citron and Frank Pasquale suggest that credit scoring software should be tested for bias and arbitrary determinations by making the datasets available to the Federal Trade Commission. They also propose making the source code and notes by the programmers on each element of the algorithms, such as the variables, correlations, and basic inferences, available for regulators' review.[177] In particular, rigorous testing can help illustrate where the translation of policy to code has gone awry.[178] Congress could establish an appropriate auditor, or mandate that the software be tested by a third party, with the results of the testing and recommendations made available to the public. Extensive training should also be required for the officers who will be expected to incorporate these algorithms into their daily work. The better officers understand how the technology operates, including the statistical probabilities it relies on and its inherent limits, the more likely it will be for them to overcome automation bias in the field.[179] Ferguson also suggests precision requirements, such that the predictions are more individualized than an amalgamation of generalized probabilities. He also recommends limits on link analysis, which illustrates broad connections between two data points; while it can point to larger, subtle patterns, it is also, by its nature, fairly generalized.[180] Others have suggested technological solutions to bridging the divide between the public's need for transparency and accountability, noting the inefficacy (and often, impossibility) of simply demanding that code be released for review.[181] Computer science researchers and social scientists have begun to focus on this problem of reluctantly encoded data and algorithms, and there have been preliminary efforts to develop methods of data mining to correct those problems, including methods that attempt to correct the bias in data before it is

174. Joh, *supra* note 50, at 31 (describing the severity of potential errors from big data in the criminal context).

175. *Id*.

176. Citron & Pasquale, *supra* note 3, at 25.

177. *Id*.

178. Jones, *supra* note 108, at 93.

179. *Id*. at 93–94.

180. *See* Ferguson, *Big Data*, *supra* note 2, at 408–09.

181. Joshua Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, *Accountable Algorithms*, 165 U. PENN. L. REV. 633, 638–40 (2017) (noting the difficulty of effective transparency in algorithmic accountability, but arguing that procedural regularity is achievable through tools like software verification and cryptographic commitments).

processed, or after the predictions are reached.[182] Such efforts could contribute to the development of non-discriminatory predictive policing, and are a key step towards developing predictive policing programs that actually deliver the increased efficiency and accuracy that they purport to create, without the deleterious compromise of discriminatory or arbitrary results.

B. Increasing Transparency in Predictive Policing

In *Technological Due Process*, Professor Danielle Citron outlines safeguards to govern the use of automated processes in administrative law to protect procedural rights such as notice and access to a fair hearing.[183] Most of these are related to transparency, such as making the source code of predictive systems open to the public and requiring audit trails.[184] The comparison of administrative and criminal justice decision-making is inexact, but the general principle applies in both cases; the better government officials, courts, and the public can understand the step-by-step deductions and decisions occurring as the technology is used, the more likely it is that the technology can be used in an accurate, legal, and ethical way. The elemental degree of transparency that should be required is awareness that the technology is being used, both on the part of the legislature and the public. Many sellers of predictive policing technology contractually require that police departments hide the use of their products, which insulates an untested and potentially problematic practice from the diagnostic clarity of public debate.[185] A risk score should be broken down into the qualitative and quantitative factors that comprise it, to the greatest degree of precision possible. An aggregated determination should never suffice as the articulable facts that can contribute to reasonable suspicion, when an officer cannot separate the distinct facts comprising

182. *See generally* Bettina Berendt & Sören Preibusch, *Better Decision Support Through Exploratory Discrimination-Aware Data-Mining: Foundations and Empirical Evidence*, 22 ARTIFICIAL INTELLIGENCE & L. 175, 175–209 (2014) (arguing for an "exploratory" approach to discovering discriminatory patterns in data mining, as opposed to constraint-oriented); Simon DeDeo, *Wrong Side of The Tracks: Big Data and Protected Categories*, *in* BIG DATA IS NOT A MONOLITH (Cassidy Sugito, Hamid Ekbia, & Michael Mattioli eds., 2015) (describing a method of encoding a decision-making process that entirely avoids correlation with protected variable, reverse-engineering algorithms to illustrate the causal relationships, and examining whether or not that could be a sufficient policy solution); Michael Feldman, Sorelle Fridler, John Moeller, Carlos Scheidegger & Suresh Venkatasubramanian, *Certifying and Removing Disparate Impact*, PROC. 21ST ACM SIGKDD INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 259, 259–68 (2015) (proposing a method to isolate and remove bias from data, while preserving relevant attributes); Koray Mancuhan & Chris Clifton, *Combating Discrimination Using Bayesian Networks*, 22 ARTIFICIAL INTELLIGENCE & L. 211, 211–38 (2014) (describing a method of isolating discrimination in a data set without using protected attributes).

183. Citron, *supra* note 3, at 1272, 1281–84.

184. *Id*. at 1284.

185. Joh, *supra* note 50, at 38 ("First, big data tools are often private market products; police departments are just another group of customers. In a number of recent instances, private companies providing surveillance technology have required agreements from police departments that prevent disclosure of information about the technology itself."); *see also supra* note 92 and accompanying text.

the determination. While transparency—of procedures, data collection, and source code—is an important safeguard against the misuse of predictive policing technology, it is still imperfect. Mandating that source code be released, for example, is an incomplete solution when few people will be capable of understanding what it means.[186] And while transparency can help reveal procedural flaws, not all of those flaws will necessarily be capable of correction, such as the institutional bias entrenched in the data, or automation bias. Transparency is necessary, but not sufficient, to counterbalance the effect of predictive policing on individual rights at the border.

C. Tailoring Predictive Policing to Realize Its Potential

While the statutory protections listed above offer a promising start to limiting the discriminatory effects of predictive policing, it remains to be seen whether they are a sufficient counterbalance to the likely effects. Nevertheless, a blanket ban, even if politically feasible, would hamper the potential of predictive policing to reduce discriminatory stops or civilian conflicts with law enforcement. The unlimited use of predictive policing algorithms will dilute the reasonable suspicion standard because it exponentially increases the volume of information that was once available to an officer in the field. However, threat scores and area-based algorithms could make otherwise overly malleable standards accountable to empirical data, thus reducing the degree of discretion capable of abuse in the reasonable suspicion standard. Statistical crime data and geographic information systems could be used to inject clarity and accountability into the highly malleable "high-crime area" determination by anchoring it to documented statistics and geographic areas; as it currently stands, the term is easily manipulated such that it can serve as a proxy for less permissible inferences based on race, criminal history, or class.[187] Meticulous recording of the events that transpire in so-called "high crime" (or high-smuggling, high trafficking) areas could allow area-based predictive policing programs to render the high-crime standard less malleable. If data is recorded on the rate of crime, and those statistics are corroborated or corrected by subsequent officer activity, the high crime area could become less subjective, and less prone to abuse.[188] Stops based on unintentional bias could be counterbalanced by exculpatory information, though if the assessments are skewed by biased intake data or the construction of the algorithm, this possibility may be limited.[189] Exculpatory risk assessments do have the potential to decrease the number of stops or searches premised on biased assumptions; the totality of

186. Kroll, Huey, Barocas, Felten, Reidenberg, Robinson & Yu, *supra* note 181, at 6.

187. Ferguson & Bernache, *supra* note 99, at 1592–93; Ferguson, *Big Data*, *supra* note 2, at 396.

188. Koss, *supra* note 88, at 334.

189. This does not strip predictive policing of all potential for discriminatory impact. In the same way that area-based algorithms will produce a feedback loop if solely predicated on historical crime data rife with racist stops, data ensuing from biased police tactics will not be an effective check.

circumstances test requires consideration of innocent facts along with incriminating ones.[190]

Were threat-scoring software sufficiently accurate, tailored, and cured of the passive discrimination encoded in the data, a score could dispel an officer's suspicion of criminal activity that may have been based on biased assumptions. A tool that could make stops at the border more accurate could protect individual rights at the border, rather than catalyzing further corrosion. Further, police activity that is driven by algorithmic prediction can then be tied to the ensuing results of each stop, and used to refine and improve the algorithm, and police activity at the border. Tracking the accuracy of stops could also highlight subtle patterns of discriminatory activity that could have otherwise gone unnoticed and uncorrected.[191] That activity could be tied to individual officers, illustrating previously unrecognized patterns of behavior, or to areas that were previously described as high crime (or high smuggling, or high trafficking).

VII.
CONCLUSION

If predictive policing technology were reliably accurate, the methodology were transparent, and law enforcement officers and judges understood its limitations, then the use of predictive policing at the border might not threaten individual rights. As it stands, the use of an unpredictable and poorly understood technology, in an area of law where a highly malleable evidentiary standard can justify a substantial intrusion on individual rights, poses a colossal problem—a problem with which the Fourth Amendment is ill-prepared to face. A blanket prohibition on the use of predictive policing algorithms is neither normatively desirable nor politically tenable, as their use could improve existing policing techniques, resulting in more effective enforcement and fewer discriminatory stops. But careful, conscientious safeguards are a precondition to harnessing the possible benefits of predictive policing algorithms, and a crucial bulwark against the risks they pose. The breathless hopes of technological evangelists must be tempered with the knowledge of technology's limits, so that the little protection there is for individual privacy and freedom at the border may be preserved.

190. Ferguson, *Big Data*, *supra* note 2, at 392.

191. *Id.*; *see generally* Sharad Goel, Maya Perelman, Ravi Shroff & David Alan Sklanky, *Combatting Police Discrimination in the Age of Big Data*, 20 NEW CRIMINAL L. REV. 181 (2017).