Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment

Michael L Rich
MACHINE LEARNING, AUTOMATED SUSPICION ALGORITHMS, AND THE FOURTH AMENDMENT

MICHAEL L. RICH

ABSTRACT

At the conceptual intersection of machine learning and government data collection lie Automated Suspicion Algorithms, or ASAs, algorithms created through the application of machine learning methods to collections of government data with the purpose of identifying individuals likely to be engaged in criminal activity. The novel promise of ASAs is that they can identify data-supported correlations between innocent conduct and criminal activity and help police prevent crime. ASAs present a novel doctrinal challenge, as well, as they intrude on a step of the Fourth Amendment’s individualized suspicion analysis previously the sole province of human actors: the determination of when reasonable suspicion or probable cause can be inferred from established facts. This Article analyzes ASAs under existing Fourth Amendment doctrine for the benefit of courts who will soon be asked to deal with ASAs. In the process, the Article reveals how that doctrine is inadequate to the task of handling these new technologies and proposes extra-judicial means of ensuring that ASAs are accurate and effective.
# Table of Contents

## Introduction

1.

## I. Machine Learning and ASAs

8.

## II. Individualized Suspicion, Old Algorithms, and ASAs

16.

   A. The Two-Step Individualized Suspicion Analysis
   
   16.

   B. Algorithms in the Individualized Suspicion Analysis: the Old and the New
   
   21.

## III. The Insufficiency of an ASA’s Prediction

24.

   A. The Collective and Constructive Knowledge Doctrines
   
   24.

   B. Applying the Doctrines to ASAs
   
   27.

## IV. ASAs as Part of the Totality of the Circumstances

34.

   A. Algorithms as Police Profiles
   
   35.

   B. Algorithms as Informants
   
   41.

   C. Algorithms as Drug-Sniffing Dogs
   
   46.

      1. The law of drug dogs
   
      48.

      2. ASAs as drug dogs
   
      55.

      3. Conclusion
   
      60.

## V. ASA Errors

62.

## VI. Conclusion

67.
INTRODUCTION

One day soon, a machine will identify likely criminal activity and, with the beep of an e-mail delivery, the buzz of an alarm, or the silent creation of a report, tell police where to find it. Already, a computer program analyzes massive quantities of securities trading data and notifies the Securities and Exchange Commission of investors who might be engaged in insider trading. Computer systems connected to networks of video cameras alert police when bags are abandoned on subway platforms or a single individual visits multiple cars in a parking structure. A device field-tested by the federal government screens individuals and predicts whether, based on physiological data, the individual intends to commit a terrorist act. Researchers at Carnegie Mellon, and funded by the Defense Advanced Research Projects Agency, are developing computer programs to index and analyze the text and images in online advertisements for sex services in order to identify sex traffickers and victims of human trafficking.

---

4 Sharon Weinberger, Terrorist “Pre-Crime” Detector Field Tested in United States, NATURE, May 27, 2011.
Technologies like these reveal the joint potential of two trends: first, the collection of massive troves of data about people in the United States; and second, the explosive growth of a field of computer science known as machine learning. With respect to the first, these data come from a nearly-unlimited variety of public and private sources, including video cameras, crime scene gunshot detectors, license-plate readers, automatic tollbooth payment systems, and social media websites. And government bodies from the municipal to the federal level are all involved in the “data vacuuming.” With a mixture of resignation and pessimism, this Article takes the government’s past and future collection of enormous quantities of personal data as a given and looks instead at the government’s use of those data.

Meanwhile, researchers have made colossal strides in recent years in machine learning, or the “the systematic study of algorithms and systems that improve their knowledge or performance with experience.” Machine learning is particularly useful for revealing complex processes.

---


7 Citron & Pasquale, supra note 6, at 1451 (discussing the range of information sources that feed into fusion centers).


9 This assumption should not suggest approval. Fortunately, more scholars than can be cited here have already discussed the panoply of concerns, often revolving around individual privacy, that this data-gathering raises.

10 Peter Flach, MACHINE LEARNING: THE ART AND SCIENCE OF ALGORITHMS THAT MAKE SENSE OF DATA 3 (Cambridge Univ. Press 2012).
that underlie observable phenomena. Machine learning techniques help computer systems “learn” the underlying process and its patterns by creating a useful approximation of how the process works. This approximation can then be used to predict future occurrences of the same phenomena. For instance, machine learning methods are used to examine patient records and create algorithms that can help doctors diagnose illnesses or provide prognoses.

At least at the conceptual level, machine learning and crime-fighting are a perfect match. The interaction of forces that cause people to commit crimes is incomprehensibly complex. Nonetheless, criminologists have sought for decades to use data to identify the most likely criminal offenders. Statistical models that aim to identify those inclined to commit crimes in the future based on quantifiable personal characteristics have become influential in the context of pretrial release, probation, and parole. Police departments have begun recently to use statistical models to predict where in their jurisdictions certain crimes are likely to occur. Machine learning provides a way to go one step further and use data to identify likely criminals among the general population of citizens without the need to disentangle the Gordian knot of causal forces.

This Article addresses such technologies that apply machine learning techniques to the “data hoards” collected by the Government in order to predict individual criminality. Some of these technologies are already in

---

11 Ethem Alpaydin, INTRODUCTION TO MACHINE LEARNING 2 (MIT Press, 2d ed. 2010).
12 Id.
13 Id.
14 See Igor Kononenko & Kukar Matjaz, MACHINE LEARNING AND DATA MINING: INTRODUCTION TO PRINCIPLES AND ALGORITHMS 25 (Horwood Publ’g 2007).
17 See Id. at 265–70 (providing examples).
18 Desai, supra note 6, at 583.
use or are in late stages of development. Nascent examples are even more numerous, including: using past offender and crime scene data to create more accurate profiles of unknown offenders, leveraging behavioral data to identify individuals who are attempting to conceal their true (and potential nefarious) intent, and analyzing past corporate financial statements to create algorithms that can determine from the language used in a financial statement whether the company is likely engaged in fraud.

This Article refers to programs like these—that are created through machine learning processes and seek to predict individual criminality—as Automated Suspicion Algorithms, or ASAs. ASAs share three defining characteristics implied by their name. First, they are based on *algorithms*, which can be broadly defined as sequences of instructions to convert some input into an output. In this case, ASAs convert data about an individual and her behavior into predictions of the likelihood that she is engaged in criminal conduct. Second, ASAs assess individuals based on suspicion of criminal activity. Third, ASAs *automate* the process of identifying suspicious individuals from data: they comb past data for factors that correlate to criminal activity, assess the weight of each factor and how it relates to other factors, use the results to predict criminality from new data, and continuously improve their performance over time. The automation of these processes distinguishes ASAs from computer systems.

---

19 See *supra* notes 1-5 for examples.
21 J.K. Burgoon et al., *Detecting Concealment of Intent in Transportation Screening*, 10 IEEE TRANSACTIONS ON INTELLIGENT TRANSP. SYSTEMS 103 (2009).
23 ALPAYDIN, *supra* note 11, at 1.
24 The fact that the processing of data is automated should not obscure the fact, however, that humans are involved in the process of programming and training the ASA. See infra § 1.
that might merely automate the application of a pre-existing police profile of criminality.  

Of course, from fingerprints to field testing kits to DNA matching, law enforcement has always tried to find ways to use the newest technologies. As a result, attorneys, judges, and commentators are quite familiar with the role that these technologies play in helping police ascertain the facts about a crime: the who, what, when, where, and why of a crime. A field test for cocaine, for instance, tells police whether a certain substance is contraband. A DNA match confirms that a suspect was at a crime scene. But determining these historical facts is only the first step in deciding whether individualized suspicion exists sufficient to justify a search or seizure.

Until now, the second step in determining the existence of individualized suspicion—determining whether the historical facts give rise to probable cause or reasonable suspicion—has remained the sole province of human actors. The Supreme Court has taught that determinations about the existence of probable cause and reasonable suspicion ultimately depend on reason, “common sense,” and police experience. Yet, the Court has also made clear that individualized suspicion is ultimately about “probabilities,” though in the next breath we learn that probabilities “are not technical.” The promise of ASAs is that they can provide data-derived probabilities of whether crime is afoot; the novel problem they

25 For instance, makers of a lighting and security system at the Newark Liberty International Airport claim that it can alert security if an individual stops at numerous cars in a parking lot, presumably because it is common wisdom in law enforcement that such behavior suggests criminal intent. Cardwell, supra note 3.


28 Id.

29 Terry v. Ohio, 392 U.S. 1, 21 (1968) (Fourth Amendment searches and seizures must be justified by facts and “rational inferences from those facts”).


present is how those statistical probabilities fit in the “practical, nontechnical conception” of individualized suspicion.33

Given that ASAs are coming,34 courts will soon be asked to consider how their output should factor into the individualized suspicion analysis.35 The initial goal of this Article is to provide courts with a framework for that analysis.36 Yet setting out this framework reveals something more. First,  

33 Id. at 176.
34 See Tal Z. Zarsky, Transparent Predictions, 2013 U.Ill. L. REV. 1503, 1506 (2013) (noting that governments “are increasingly curious to figure out what we will do next and take action, rather than wait and investigate what has already happened and suffer the possible consequences”); Reed E. Hundt, Making No Secrets About It, I/S: J. L. & POL’Y FOR INFO. SOC’Y 581, 588 (2014) (asserting that “government now routinely asks computers to suggest who has committed crimes”). Though the author has found no reported case that addresses this issue, the Virginia Supreme Court came tantalizingly close in Commonwealth v. Smith, 281 Va. 582 (2011). There, officers conducted a Terry frisk of a suspect solely on the basis of an alert they received from a police database known as PISTOL (Police Information System Totally On Line) that stated that the suspect was “probably armed and a narcotics seller/user.” Id. at 591. The alert issued because an officer had made a record in the system of the suspect’s prior arrest for weapons and drug crimes. Id. The lower court record did not reveal whether the alert issued because of an automated decision of the PISTOL software or the choice of the officer who created the earlier arrest record. Smith v. Commonwealth, 55 Va. App. 30, 34 n.1 (Va. Ct. App. 2009), rev’d 281 Va. 582 (2011). Regardless, the Virginia Supreme Court relied upon the constructive knowledge doctrine, discussed infra § III.A, in refusing to suppress evidence obtained as a result of the frisk. Smith, 281 Va. at 591-92.
35 The Fourth Amendment implications of automated predictions about the criminality have largely escaped in-depth analysis by scholars, though some have recognized the importance of the question. One is Daniel J. Steinbock, Data Matching, Data Mining, and Due Process, 40 GA. L. REV. 1 (2005), who raises, but does not answer, the overarching question discussed herein. See id. at 30. Another is Murphy, supra note 26, who frames the issue as “the challenges that large-scale databasing pose[] to conventional constitutional analysis.” Id. at 804. Her discussion of issues raised by databases is extremely useful in the context of ASAs, but she does not attempt to examine the individualized suspicion analysis in any depth. See id. at 826 (“[M]y aim is more to think about the meaning of databases than the meaning of constitutional doctrine.”). Finally, Andrew David Ferguson asks, but again does not resolve, many of the questions addressed herein. See Andrew Guthrie Ferguson, Big Data and Predictive Reasonable Suspicion, 163 U. PA. L. REV. 327, 383–87 (2015).
36 As the discussion herein ultimately concludes, see § VI, courts are likely not the best place for rule-making with respect to ASAs. See Orin S. Kerr, The Fourth
we learn that ASA’s push the limits of the Court’s current approach to the Fourth Amendment in areas that have already raised red flags among scholars. One area is the ongoing metamorphosis of the collective knowledge doctrine into what some call the “constructive knowledge” doctrine.\(^37\) The former allows knowledge to be imputed between officers, so one officer may instruct another to conduct a search or seizure without having to explain why.\(^38\) The latter permits a search based on the aggregated knowledge of law enforcement personnel generally, even if no one officer possessed enough knowledge to make an individualized suspicion assessment.\(^39\) Another relevant area of concern is the integration of statistical data in the individualized suspicion analysis,\(^40\) which the Supreme Court recently tackled in the context of drug dogs.\(^41\) A third area implicated by ASAs is the Supreme Court’s holding that errors in police databases require the exclusion of evidence only in cases of gross negligence or systemic misconduct.\(^42\) Taken together, these issues reveal a second, overarching point: that ASA accuracy cannot be regulated through the courts alone; rather, extra-judicial action is needed to ensure

---


38 Stern, supra note 37, at 1086.

39 Id. at 1087.

40 See, e.g., Erica Goldberg, Getting Beyond Intuition in the Probable Cause Inquiry, 17 LEWIS & CLARK L. REV. 789 (2013) (discussing the errors that often arise when courts attempt to incorporate statistical data in the individualized suspicion determination); Richard E. Myers, Detector Dogs and Probable Cause, 14 GEO. MASON L. REV. 1 (2006) (explaining how misunderstandings about the accuracy of a drug dog’s alert leads courts to ascribe them more evidentiary value than they deserve).


that ASAs are created, maintained, used, and updated accurately and effectively.

Part I provides a brief background of machine learning and how it could be applied to create ASAs. Part II sketches out the Fourth Amendment’s individualized suspicion analysis, with a particular focus on the two steps articulated by the Supreme Court. Part III tackles the question of whether an ASA’s prediction can be sufficient to establish individualized suspicion and concludes that it cannot. Part IV discusses how ASAs should be integrated into the totality of the circumstances analysis. Part V addresses how courts should handle ASA errors, and specifically when such errors should lead to exclusion of evidence. Part VI concludes by pulling together lessons from the prior discussion and proposing extra-judicial ways to ensure ASA accuracy.

I. MACHINE LEARNING AND ASAS

“Machine learning” is part of a nest of concepts in the artificial intelligence arena, including “data mining,” “knowledge discovery in databases,” and “big data,” that are often used interchangeably and confusingly within academia, the government, and popular media.43 For the sake of clarity, mentions of “machine learning” in this Article refer to the study of algorithms that analyze data in order to help computer

43 For instance, Daniel Solove calls the process undertaken by algorithms like ASAs “data mining.” See Daniel J. Solove, Data Mining and the Security-Liberty Debate, U. CHI. L. REV. 343, 343 (2008) (“Data mining involves creating profiles by collecting and combining personal data, and analyzing it for particular patterns of behavior deemed to be suspicious.”). That term is not used herein, however, because it is not consistently defined in the literature, see, e.g., Jeffrey W. Seifert, Data Mining and the Search for Security, 21 GOV’T INFO. Q. 461, 462 (2004) (“[W]hile data mining is widely mentioned in a growing number of bills, law, reports, and other policy documents, an agreed upon definition or conceptualization of data mining appears to be generally lacking within the policy community.”), and it fails to capture the pattern detection that is crucial in the criminal law context. This Article does not undertake the Herculean task of resolving the terminological confusion, though others have done so. See Liane Colonna, Taxonomy and Classification of Data Mining, 16 SMU SCI. & TECH. L. REV. 309, 313–29 (2013) (defining a wealth of terms relating to machine learning and data mining).
systems become more accurate over time when completing a task.\textsuperscript{44} This continuous improvement on a given task is the “learning” referenced in “machine learning,” as opposed to the more holistic concept referred to when people speak of human learning.\textsuperscript{45} In particular, machine learning does not require a computer to engage in higher-order cognitive skills like reasoning or the understanding of abstract concepts.\textsuperscript{46} Rather, machine learning applies inductive techniques to often-large sets of data to “learn” rules that are appropriate to the task.\textsuperscript{47} In other words, the “intelligence” of a machine learning algorithm is oriented to outcomes not process: a “smart” algorithm reaches consistently accurate results even if algorithm does not “think” like a person.\textsuperscript{48}

Machine learning methods are particularly good at helping computers look at a complex set of data and model the underlying processes that generated those data.\textsuperscript{49} The models generated through this process can then be applied to new data in order to predict outcomes.\textsuperscript{50} One of the most common tasks undertaken by machine learning algorithms is the “classification” of “objects,” a catchall concept that can include anything, including people, about which one might collect data.\textsuperscript{51} Classification is an example of what is called “supervised” machine learning, in which an algorithm learns from data that has already been “labelled” with the target feature.\textsuperscript{52} “Features” are the “language” that machine learning algorithms

\textsuperscript{44} See id. at 320 ("[M]achine learning is concerned with the development of algorithms and techniques for building computer systems that can automatically improve with experience...."); Harry Surden, Machine Learning and Law, 89 WASH. L. REV. 87, 89 (2014) ("Machine learning' refers to a subfield of computer science concerned with computer programs that are able to learn from experience and thus improve their performance over time."); FLACH, supra note 10, at 3 ("Machine learning is the systematic study of algorithms and systems that improve their knowledge or performance with experience.").
\textsuperscript{45} Surden, supra note 44, at 89.
\textsuperscript{46} Id. at 94–95.
\textsuperscript{47} Id. at 91 n.21.
\textsuperscript{48} Id. at 95–96.
\textsuperscript{49} KONONENKO & MATJAZ, supra note 14, at 1.
\textsuperscript{50} ALPAYDIN, supra note 11, at 2.
\textsuperscript{51} See FLACH, supra note 10, at 13–14.
\textsuperscript{52} Id. at 14. Alternatively, machine learning can occur in an “unsupervised” or “semi-supervised” environment, where all or much of the data used to train an algorithm is
uses to describe the objects within its domain. The only technological limit on the kind of characteristic that can be a feature is that it must be measurable. The machine learning process then creates a “model” based on this data that can be used to predict the proper classification of future objects.

Machine learning methods are already used in a wide variety of classification tasks, including the identification of “spam” e-mails, optimization of productions processes, the diagnosis of diseases, risk evaluation, image classification, and game playing. A primary task of law enforcement in ferreting out crime is also one of classification:

unlabeled. Id.; Steven M. Bellovin et al., When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning, 8 N.Y.U. J. L. & LIBERTY 556, 590–96 (2014) (providing an overview of unsupervised, supervised, and semi-supervised machine learning approaches). In the law enforcement context, this would mean that machine learning methods are used to examine data about individuals where it is unknown whether the individual is engaged in criminal conduct. In such a case, a machine learning algorithm may engage in “clustering,” by which similar instances are grouped together and the attributes of that group are defined. ALPAYDIN, supra note 11, at 155. Then, a law enforcement expert may use the groupings to gain a better understanding of a given population and develop appropriate strategies for each group. See id. (discussing a similar strategy in the context of a commercial enterprise analyzing its customer base). Police already interact with groups differently based on assumptions about their likelihood to engage in criminal conduct. See, e.g., Wendy Ruderman, To Stem Juvenile Robberies, Police Trail Youths Before the Crime, N.Y. TIMES, Mar. 4, 2013, at A1 (reporting on New York City Police Department project to conduct early intervention with juveniles who are believed to be likely to engage in violent crime). The Fourth Amendment typically requires individualized suspicion based on something more than group membership, however. David A. Harris, Using Race or Ethnicity as a Factor in Assessing the Reasonableness of Fourth Amendment Activity: Description, Yes; Prediction, No, 73 MISS. L.J. 423, 442 (2003). Thus, this Article will focus on supervised machine learning ASAs, which is more likely to be able to provide the required individualized suspicion. Nonetheless, many of the insights unearthed herein would also apply to unsupervised machine learning.

53 FLACH, supra note 10, at 13.
54 Id. at 38–39.
55 Id. at 13, 17.
56 See id. at 1–12 (discussing “spam” identification in detail); ALPAYDIN, supra note 11, at 4–14 (providing examples); KÖNONENKO & MATJAZ, supra note 14, at 24–29 (same).
distinguishing the guilty from the innocent.⁵⁷ Or, more precisely in the Fourth Amendment context, the job of the police officer is to separate the likely criminals from the unlikely.⁵⁸ Thus, the machine learning task of classification is an ideal complement to the police officer’s job. An ASA would begin with historical data about people containing a wide variety of features that might be relevant to predicting different kinds of criminal activities, including immutable personal characteristics (e.g., age, gender, race, religion), demographic information (e.g., address, salary, occupation), or specific activities of the individuals (e.g., presence on a certain street corner at a certain time, patterns of flights, or specifics of tax returns).⁵⁹ These data would also be labelled, indicating whether each included person was engaged in the targeted criminal conduct or not. Machine learning methods would then be applied to these data to create a model that the ASA could then apply to new data in order to predict which individuals are likely to be engaged in the targeted criminal activity.

A somewhat deeper understanding of the supervised machine learning process will be helpful to the Fourth Amendment analysis.⁶⁰ In supervised machine learning, the initial set of labelled data is typically subdivided into three sets: a “training set,” a “verification set” or

⁵⁷ See JEROME H. SKOLNICK, JUSTICE WITHOUT TRIAL: LAW ENFORCEMENT IN A DEMOCRATIC SOCIETY 196–97 (John Wiley & Sons, Inc. 1966) (discussing police perception of expertise in distinguishing the guilty from the innocent).
⁵⁸ See Hill v. California, 401 U.S. 797, 804 (1971) (“[S]ufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment....”).
⁵⁹ While there would be legal limits on the use of some personal characteristics as features in an ASA, such as the Equal Protection Clause’s ban on intentional discrimination, the Fourth Amendment does not impose any appear to impose any such restriction. See Whren v. United States, 517 U.S. 806, 813, 817 (1996) (“We of course agree with petitioners that the Constitution prohibits selective enforcement of the law based on considerations such as race. But the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment.”).
⁶⁰ This discussion is only a high-level overview of a deep and complex field of mathematics. It does not, and is not intended to, comprehensively discuss all the issues that might arise in the construction of an ASA; rather, it aims to highlight some substantial concerns and identify the sort of information that might be helpful in identifying others.
“validation set,” and a “test set.” During the development of a model, the algorithm first learns an initial group of classification rules by analyzing the training set. These rules are then applied to a validation or verification set, and the results are used to optimize the rules’ parameters. Finally, the optimized rules are applied to the test set, and the results establish both a “confidence” level and a “support” level for each rule. The support level of a rule describes the percentage of objects in the test set to which the rule applies. Rules with a low support level are less likely to be statistically significant. Thus, programmers set a minimum support level for rules that the algorithm will apply to ensure that predictions are made only on the basis of statistically significant correlations. The confidence level of a rule describes how often objects in the test set follow the rule. The confidence level is, in essence, a measure of the strength of the algorithm’s prediction. Thus, a 70% confidence level would allow an ASA to predict that there is a 70% chance that a suspect meeting the rule in question is engaged in criminal conduct.

Machine learning algorithms are not perfect, of course, and mistaken predictions can result from four general sources of inaccuracy. First, when machine learning methods are used to model complex causal systems, they rely upon approximations. The causes of criminal conduct are of sufficient complexity to motivate entire fields of study, but the ASA does not become a criminologist, psychologist, police officer, or

---

61 See FLACH, supra note 10, at 50; ALPAYDIN, supra note 11, at 39–40; KONONENKO & MATJAZ, supra note 14, at 85.
62 FLACH, supra note 10, at 50.
63 KONONENKO & MATJAZ, supra note 14, at 85.
64 See FLACH, supra note 10, at 182–84 (explaining the creation of association rules, such as rules that associate certain facts to criminal conduct).
65 Id. at 182.
66 Zarsky, supra note 34, at 1525. It is possible, though, for a rule with a low support level to be statistically significant. Id.
67 Zarsky, supra note 34, at 1525.
68 FLACH, supra note 10, at 184.
69 Surden, supra note 44, at 97; see ALPAYDIN, supra note 11, at 2 (“We may not be able to identify the process completely, but we believe we can construct a good and useful approximation. That approximation may not explain everything, but may still be able to account for some part of the data.”).
sociologist. Instead, the machine learning methods use patterns, and correlations within the data to create a model that differentiates criminals from non-criminals.\textsuperscript{70} Because these patterns and correlations are mere estimates of the more complex underlying phenomenon, they are inevitably inaccurate in some instances.\textsuperscript{71} The inaccuracies can be reduced, however, if the set of training data is large and representative.\textsuperscript{72}

Second, inaccuracies in supervised machine learning models may come from “noise” in the training data.\textsuperscript{73} In other words, the training data may contain information about the people described therein that is wrong. For instance, a database containing the training data for an ASA targeting auto theft may list each individual’s age. The database may say a particular individual was 30 years-old when she was really 40 years-old, or perhaps the database says that this individual was engaged in auto theft when she really was not. Though these kinds of noise differ in terms of their source,\textsuperscript{74} they both can cause the machine learning process to create inaccurate algorithms.\textsuperscript{75} Inaccuracies resulting from noise can be mitigated by avoiding “overfitting,” or trying to match the algorithm perfectly to the training data, and by the use of test sets that were not used to train the algorithm.\textsuperscript{76}

Third, inaccuracies can arise if an algorithm’s training data is not representative of occurrences of the relevant event or object in the

\textsuperscript{70} See id. (discussing how machine learning uses a “strategy that has proven to be successful in automating a number of complex tasks: detecting proxies, patterns, or heuristics that reliably produce useful outcomes in complex tasks that, in humans, normally require intelligence.”).

\textsuperscript{71} Id. at 98.

\textsuperscript{72} See id. at 105–6 (“Additionally, machine learning algorithms often require a relatively large sample of past examples before robust generalizations can be inferred. To the extent that the number of examples (e.g., past case data) are too few, such an algorithm may not be able to detect patterns that are reliable indicators.”).

\textsuperscript{73} ALPAYDIN, supra note 11, at 30–31; FLACH, supra note 10, at 50.

\textsuperscript{74} The former is called instance noise, and the latter is called label noise. FLACH, supra note 10, at 50.

\textsuperscript{75} Avoiding inaccuracies resulting from noise can be mitigated by

\textsuperscript{76} FLACH, supra note 10, at 50.
world.\textsuperscript{77} For instance, if our ASA that is meant to identify likely auto theft is trained on data only from a single city, the ASA will not less accurate when applied nationally if auto thieves have different criminal methods in different locales. Similarly, machine learning methods typically assume that the near future will be substantially similar to the time when the sample data was collected.\textsuperscript{78} Thus, if the methods of auto thieves change over time, perhaps in response to police action or new technologies, our ASA seeking to identify them will become less accurate unless the ASA is constantly learning from new data.

Fourth, the choices made by humans throughout the machine learning process can cause inaccuracies in the final predictions of a machine learning algorithm.\textsuperscript{79} At the outset, decisions must be made about what features of the objects in question should be used to construct the model.\textsuperscript{80} In other words, before an ASA can be developed, a person must decide what facts might matter in determining whether certain behavior or characteristics are indicative of criminal conduct and how that fact might be described. For example, if an ASA is meant to detect suspicious bank transactions, should we look at the timing of each transaction? If so, is it the time of day that matters, the temporal distance of the transaction from other similar transactions, or some other time-related characteristic? The selection of the features to be analyze is “absolutely crucial” to the success of the machine learning process.\textsuperscript{81} Next, data analysts must construct the training dataset.\textsuperscript{82} This requires decisions about which databases to use, how to normalize data from different databases so that all the objects are described in terms of the same set of features, and whether to reject data that a given analyst believes is wrong or insignificant.\textsuperscript{83} These decisions and others allow human assumptions about what correlations should exist

\begin{itemize}
\item \textsuperscript{77} See \textit{Id.} at 55 ("We typically only have access to the true classes of a small fraction of the instance space and so an estimate is all we can hope to get. It is therefore important that the test set is as representative as possible."); Surden, \textit{supra} note 44, at 106.
\item \textsuperscript{78} ALPAYDIN, \textit{supra} note 11, at 2.
\item \textsuperscript{79} Zarsky, \textit{supra} note 34, at 1518–19; see also Colonna, \textit{supra} note 43, at 335–37 (discussing the role of various human actors in a data mining process).
\item \textsuperscript{80} FLACH, \textit{supra} note 10, at 41.
\item \textsuperscript{81} \textit{Id.}
\item \textsuperscript{82} Zarsky, \textit{supra} note 34, at 1518.
\item \textsuperscript{83} \textit{Id.}
\end{itemize}
in the data to color the outcome. The algorithm must then be trained, a process that requires, among other things, a decision about how different kinds of potential errors should be weighted. For instance, someone must decide in the ASA context whether it is worse for an innocent person to be treated like a likely criminal or for a criminal to be ignored by the police, and if so, how much worse. This decision will push the resulting model toward either higher or lower predictions of criminality. Finally, once an algorithm is generated, a person must answer numerous questions about how it is applied in the field. For example, how certain must a prediction be before it is reported to the police and what information will the ASA convey to the police about the prediction? All of these decisions will impact a model’s accuracy and operation when it is put into practice.

A decision also must be made about whether to make a machine learning algorithm interpretable. A model’s interpretability describes the extent to which a machine learning algorithm’s analysis of data is understandable to humans. Absent an intentional decision to the contrary, machine learning tends to create models that are so complex that they become “black boxes,” where even the original programmers of the algorithm have little idea how or why the generated model creates accurate predictions. On the other hand, when an algorithm is interpretable an outside observer can understand what factors the algorithm relies on to make its predictions and how much weight it gives to each factor. Interpretability comes at a cost, however, as an interpretable model is necessarily simpler and thus often less accurate than a black box model.

---

84 See id. at 1552 (noting that “human decisions carry particularly risks of their own—such as hidden and internal biases that might be premised upon bigotry”).
85 KONONENKO & MATJ AZ, supra note 14, at 71.
86 See, e.g., Richard Berk, Algorithmic Criminology, 2 SECURITY INFORMATICS 5, 8 (2013) (assuming in the probationary context a cost ratio between false negatives and false positives of 20 to 1).
87 See Zarsky, supra note 34, at 1519.
88 Id. at 1566.
90 ALPAYDIN, supra note 11, at 197–98.
91 Zarsky, supra note 34, at 1520.
II. INDIVIDUALIZED SUSPICION, OLD ALGORITHMS, AND ASAS

This section lays out the existing doctrine that governs the finding of individualized suspicion to justify either a search or seizure under the Fourth Amendment. First, it articulates the two sequential steps that a police officer, magistrate, or court must undertake when determining whether probable cause or reasonable suspicion exists in a given case. The section then establishes that ASAs play a different role in the individualized suspicion analysis than traditional algorithmic data.

A. The Two-Step Individualized Suspicion Analysis

In most circumstances, the police must have individualized suspicion that a person is engaged in criminal conduct before they can search or seize that person. The two prototypical levels of individualized suspicion are reasonable suspicion, which is required to conduct a limited search or brief seizure as articulated in *Terry v. Ohio*, and probable cause, which is required for a “full-blown” arrest or more intrusive search. To determine whether individualized suspicion exists, courts and police must look at “the totality of the circumstances—the whole picture.” The Court adopted the totality-of-the-circumstances approach in *Illinois v. Gates* to overturn a line of precedent that had been interpreted

---

92 Though the Court has authorized suspicionless searches and seizures to serve "special needs, beyond the normal need for law enforcement," *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000) (internal quotations omitted), the focus in this Article is on policing that serves typical crime-prevention goals.


94 392 U.S. 1 (1968).

95 *Id.* at 19-20.

to limit when anonymous tips could be used to establish probable cause.\footnote{462 U.S. at 233.}

The Court instructed that rather than applying “rigid legal rules” in the individualized suspicion analysis, police and magistrates must engage in a “balanced assessment of the relative weights” of all the relevant evidence.\footnote{Id. at 232, 234.} In a similar vein, the totality-of-the-circumstances approach requires police and magistrates to consider exculpatory evidence, along with any incriminating facts, in determining whether individualized suspicion exists.\footnote{See Gardenshire v. Schubert, 205 F.3d 303, 318 (6th Cir. 2000) ("A police officer has probable cause only when he discovers reasonably reliable information that the suspect has committed a crime. And, in obtaining such reliable information, an officer cannot look at the evidence of guilty while ignoring all exculpatory evidence.") (citation omitted); Broam v. Bogan, 320 F.3d 1023, 1032 (9th Cir. 2003) ("An officer is not entitled to a qualified immunity defense, however, where exculpatory evidence is ignored that would negate a finding of probable cause."); Wilder v. Turner, 490 F.3d 810, 814 (10th Cir. 2007) ("We determine probable cause from the totality of the circumstances taking into account both inculpatory as well as exculpatory evidence.").}

The totality-of-the-circumstances analysis involves two distinct, sequential steps:

The principal components of a determination of reasonable suspicion or probable cause will be [(1)] the events which occurred leading up to the stop or search, and then [(2)] the decision whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to reasonable suspicion or to probable cause.\footnote{Ornelas v. United States, 517 U.S. 690, 696 (1996).}

The “events which occurred leading up to the stop or search” answer basic who, what, where, and when questions about the crime and the suspect: Who is she? What did she do? Where is she? When did she engage in the relevant conduct?\footnote{Id.}

The sources of this information are as diverse as human experience would suggest: direct observation by law enforcement personnel, tips from informants, and documentary evidence
are but a few. The question for an officer, magistrate, or court at this stage is relatively straightforward: was the information that law enforcement had sufficiently reliable for a reasonable officer to rely upon it in determining the historical facts?¹⁰² The methods used to evaluate the reliability of a given piece of evidence differ depending on the nature of the evidence, of course, and the evaluation can be quite difficult. Nonetheless, courts have extensive experience with such questions.¹⁰³

The second step is more complicated because it presents a mixed question of law and fact.¹⁰⁴ An officer, magistrate, or court must decide, given the historical facts upon which a reasonable officer would rely, “whether the facts satisfy the relevant [] constitutional standard.”¹⁰⁵ Determinations about what behavior is adequately indicative of criminal conduct must be “practical [and] commonsense”¹⁰⁶ and based upon “inferences about human behavior.”¹⁰⁷ In addition to historical facts, these inferences may be informed by “background facts” about the community at issue that are unlikely to be the subject of proof.¹⁰⁸ Courts are also instructed to defer to police experience and training in deciding whether individualized suspicion exists. For instance, the Court in United States v. Brignoni-Ponce recognized that “the officer is entitled to assess the facts in light of

¹⁰² See Illinois v. Rodriguez, 497 U.S. 177, 185 (1990) (“what is generally demanded of the many factual determinations that must regularly be made by agents of the government... is not that they always be correct, but that they always be reasonable”).
¹⁰³ As just one example, the question of how to assess the reliability of an informant has long occupied both courts and commentators. For instance, according to Westlaw the Supreme Court’s decision in Illinois v. Gates, 462 U.S. 213 (1983), has been cited by courts more than 3,200 times for the proposition that corroboration of an informant’s tip is an important factor in establishing the tips reliability.
¹⁰⁵ Id. (internal quotation omitted).
¹⁰⁸ For instance, in Ornelas, police stopped the occupants of a car with California license plates at Milwaukee hotel in December. 517 U.S. at 691-92. The Court argued that background facts like the geographical location of Milwaukee and the meteorological conditions there in the winter permitted the inference that the defendants were not on vacation, but rather were in the city either to conduct business or visit family or friend. Id. at 699.
his experience” detecting the criminal conduct at issue.\textsuperscript{109} In \textit{United States v. Arvizu}, the Court reiterated that the individualized suspicion analysis “allows officers to draw from their own experience and specialized training to make inferences from and deductions about cumulative information available to them that ‘might well elude an untrained person.’”\textsuperscript{110} Taken together, these rulings teach that the level of suspicion arising from a given set of facts “may vary depending on what a police officer knew based on her training, experience, and familiarity with the neighborhood.”\textsuperscript{111}

The Court’s guidance on the inference of suspicion from historical facts leaves numerous ambiguities unresolved. First, the Court has intentionally failed to state precisely how likely criminal conduct must be to satisfy the reasonable suspicion and probable cause standards. The individualized suspicion analysis “does not deal with hard certainties, but with probabilities,”\textsuperscript{112} yet the Court has rejected any attempts to quantify the relevant probabilities.\textsuperscript{113} Second, courts and police have little guidance on how to weigh various kinds of data in deciding whether individualized suspicion exists. Because the hard questions of suspicion involve predicting criminal conduct from non-criminal behavior, “the relevant inquiry is not whether particular conduct is ‘innocent’ or ‘guilty,’ but the degree of suspicion that attaches to particular types of noncriminal acts.”\textsuperscript{114} Yet courts rarely possess empirical data that might prove or

\textsuperscript{109} 422 U.S. 873, 885 (1975).
\textsuperscript{113} See Maryland v. Pringle, 540 U.S. 366, 371 (2003) (“The probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances.”). \textit{See also} Goldberg, \textit{supra} note 40 (calling for the establishment of a minimum numerical threshold for probable cause).
disprove a correlation between certain conduct and criminal activity.\textsuperscript{115}

And even when they do, courts are typically untrained in how to assess that data.\textsuperscript{116} Finally, the Supreme Court has not explained how courts

\textsuperscript{115} E.g. Illinois v. Wardlow, 528 U.S. 119, 124-25 (2000) (“In reviewing the propriety of an officer’s conduct, courts 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 officials where none exists.”); see Tracey L. Meares & Bernard E. Harcourt, \textit{Transparent Adjudication and Social Science Research in Constitutional Criminal Procedure}, 90 J. CRIM. L. & CRIMINOLOGY 733, 750-52 (2000); David Rudovsky & Lawrence Rosenthal, \textit{Debate: The Constitutionality of Stop-and-Frisk in New York City}, 162 U. PA. L. REV. ONLINE 117, 119 (2013) (“The Court has not required police or prosecutors to demonstrate by empirical data that the characteristics relied upon—for example, that the suspect was acting suspiciously, had fled from police, had bulges in his pockets, or was engaged in ‘furtive movements’—are actually predictive of criminal conduct.”); Andrew E. Taslitz, \textit{Cybersurveillance Without Restraint?}, 103 J. CRIM. L. & CRIMINOLOGY 839, 862–63 (2013).

\textsuperscript{116} For instance, in \textit{Navarette v. California}, 134 S. Ct. 1683 (2014), the Supreme Court asked whether a reliable tip that a truck had nearly run another vehicle off the road created reasonable suspicion that the driver of the truck was intoxicated. \textit{Id.} at 1690. In concluding that it did, the Court relied on a pamphlet on the visual detection of impaired motorists issued by the National Highway Traffic Safety Administration. \textit{See id.} at 1691 (citing Nat. Highway Traffic Safety Admin., \textit{The Visual Detection of DWI Motorists} 4-5 (Mar. 2010), available at http://nhtsa.gov/staticfiles/nti/pdf/808677.pdf (visited on February 27, 2015). This pamphlet lists probabilities that a driver exhibiting certain behaviors, including “almost striking a vehicle or other object,” is intoxicated. Nat. Highway Traffic Safety Admin., \textit{supra} at 5. The pamphlet is light on an explanation of the foundation for its claimed probabilities, however. \textit{See Nat. Highway Traffic Safety Admin., \textit{supra} note \_} at 4 (stating only that the pamphlet is based on a prior NHTSA study and “3 field studies involving hundreds of officers and more than 12,000 enforcement stops”). Yet the Court seemed unconcerned with exploring the reliability of this statistical information, despite the weight that the Court placed on the pamphlet. \textit{See Navarette}, 134 S. Ct. 1683, 1691 (relying on the NHTSA pamphlet to conclude that running another car off the highway “bears too great a resemblance to paradigmatic manifestations of drunk driving to be dismissed as an isolated example of recklessness”). A comparison of the Court’s questioning of the available data with the analysis of the same data by Joshua C. Teitelbaum, \textit{Probabilistic Reasoning in Navarette V. California}, 62 UCLA L. REV. DISC. 158 (2014), reveals the shallowness of Court’s examination.
should decide whether to defer to police experience in a given case and how much deference to give.  

B. Algorithms in the Individualized Suspicion Analysis: The Old and the New

Law enforcement officials have used the output of automated algorithms for decades. Breathalyzers run on algorithms that state the amount of alcohol in an individual’s blood based on the alcohol in a sample of that individual’s breath. Radar guns send radio waves at a certain frequency in the direction of a moving automobile, measure the frequency of reflected waves that return, and calculate the speed of the automobile based on the change in frequency. A DNA sample from a crime scene can be matched against stored DNA profiles using search algorithms. And emerging algorithmic biometric technologies aim to enhance the ability of police to identify suspects and track their movements.

117 See L. Song Richardson, Police Efficiency and the Fourth Amendment, 87 Ind. L.J. 1143, 1155 (2012) (noting that “courts consistently fail to determine whether the inferences drawn by the officer conducting the stop are actually entitled to any weight”).


120 See Ryan V. Cox & Carl Fors, Admitting Light Detection and Ranging (LIDAR) Evidence in Texas: A Call for Statewide Judicial Notice, 42 St. Mary’s L.J. 837, 842-43 (2011). The other main speed detection device, known as a LIDAR gun, use a simple algorithm to calculate the speed of an automobile based on the time it takes repeated pulses of light to reflect back to the device. Id. at 849.


122 See Margaret Hu, Biometric ID Cybersurveillance, 88 Ind. L.J. 1475, 1500–1508 (2013).
These traditional technologies can be exceptionally helpful to police in establishing the “historical facts” of what happened, when it happened, and who was involved. In the case of DNA matching, algorithmic searches of databases reveal either who was at the scene of a given crime or whether a given person was at the scene of other unsolved crimes. Radar guns tell how fast a vehicle is moving at a given moment. Newer biometric technologies can provide substantially more information about a suspect’s location and movements. All of these technologies help police establish facts that can be ascertained to a definable level of certainty: a driver had a quantity of alcohol in his bloodstream that is certain to within some calibration level or the DNA found at a crime scene matches a specific person to some statistical level of confidence. And because these technologies answer questions of fact, a court can focus its analysis on the familiar issue of the accuracy of the technology used to determine the fact at issue.

The output of an ASA, on the other hand, is directed only at the mixed question of law and fact of whether the historical facts are sufficient to establish reasonable suspicion or probable cause. An ASA could be incorporated into a larger computer system that collects data, which is then fed into the ASA. Nonetheless, for the sake of analytical precision, these two functions should be considered separately.

---

125 See Hu, supra note 122. at 1490-91 (discussing “identity verification” and “identity determination” systems).
126 See, e.g., People v. Nelson, 185 P.3d 49, 53-54 (Cal. 2008) ("[T]he prosecution presented evidence that the DNA profile on the vaginal swab would occur at random among unrelated individuals in about one in 950 sextillion African-Americans, on in 130 septillion Caucasians, and one is 930 sextillion Hispanics.").
128 An ASA could be incorporated into a larger computer system that collects data, which is then fed into the ASA. Cf. Cardwell, supra note 3. (discussing a computer system that would both record video images and analyze them to decide whether crime is likely occurring). Nonetheless, for the sake of analytical precision, these two functions should be considered separately.
certain set of “features” is engaged in criminal conduct. In providing a prediction of criminality, the ASA’s examination of data overlaps with the second step in the individualized suspicion analysis. As such, ASAs provide a kind of data to the Fourth Amendment analysis that serves an analytically different role than the output of traditional algorithms.

Consider the case of People v. Nelson, from the California Supreme Court. In Nelson, a nineteen year-old college student disappeared after telephoning her mother to report that her car would not start. The victim’s body was found two days later. After more than twenty-five years, police arrested the defendant after DNA collected from the victim’s body and sweater was found to match a sample obtained from him and placed in a state database. Unsurprisingly, the DNA match was important enough to the case that its admissibility was a central question on the appeal of defendant’s conviction. Yet, the DNA match, standing alone, could only establish, albeit with great confidence, certain historical facts about the victim’s death; it could not tell police how likely it was that the defendant was guilty. Imagine, for a moment, that the police have a murder and a DNA sample that incontrovertibly matches a suspect. Those two facts, no matter how strongly established, say nothing about the likelihood that the suspect committed the murder. Rather, to connect the suspect to the murder, we (and the police) must know more. In Nelson, that “more” included: that the victim had been raped before she was killed, that the DNA sample was collected from semen on her body and clothing, and that the victim was seen in a car matching one owned by the defendant shortly before her death. Only when considering these facts together can we conclude that there is a high probability that defendant killed the

129 This term is used in the technical sense described above, see supra notes 53-54 and accompanying text, not in reference to the physical features of a suspect.
130 See Brinegar v. U.S., 338 U.S. 160, 175 (1949) (“In dealing with probable cause, however, as the very name implies, we deal with probabilities.”).
131 The extent of the overlap is discussed infra § III.
132 185 P.3d 49 (Cal. 2008).
133 Id. at 53.
134 Id.
135 Id.
136 See id. at 59-66.
137 Id. at 53.
victim. The novelty of an ASA, as distinct from technologies like DNA matching, is that the ASA can consider groups of facts together and draw conclusions about the probability of an individual’s guilt.

III. The Insufficiency of an ASA’s Prediction

Say that an ASA predicts a 60% likelihood that a specific person is selling drugs on a street corner, and a police officer, upon receiving the prediction, stops the suspect, frisks him, and finds drugs. If the defendant challenges the stop and frisk, can the prosecution rely solely on the ASA’s prediction, or does the Fourth Amendment require something more? The “collective knowledge” doctrine, which allows one police officer to engage in a search or seizure based on the instruction of another officer who knows facts that establish individualized suspicion, provides a framework for answering this question. If the ASA’s prediction is the equivalent of an officer’s instruction, then an officer is justified in acting on that prediction, standing alone. The first part of this section lays out the scope and operation of the collective knowledge doctrine, including how some courts have extended the doctrine to apply to constructive knowledge, and scholars’ criticisms of the expanded doctrine. The second explores the application of the doctrine to an ASA’s output. The section concludes first that the expanded “constructive knowledge” doctrine, as applied to ASAs, would eviscerate the individualized suspicion requirement. Second, this section establishes that an ASA’s prediction is not sufficient to create individualized suspicion.

A. The Collective and Constructive Knowledge Doctrines

In Whiteley v. Warden, Wyoming State Penitentiary, the Court held that when one officer asks another officer to help her with the execution of a warrant, the second officer is entitled to presume that the first officer provided a magistrate with sufficient information to justify a finding of probable cause. The Court expanded this rule in United States v. Hensley beyond situations involving a warrant to allow an officer to

---

138 United States v. Lyons, 687 F.3d 754, 766 (6th Cir. 2012).
139 401 U.S. 560 (1971).
140 Whiteley, 401 U.S. at 568.
rely on a flyer or bulletin if: (1) the officer acted in “objective reliance” on the flyer or bulletin; and (2) the flyer or bulletin was based on articulable facts sufficient to establish the necessary individualized suspicion. Lower courts have since applied the collective knowledge rule to justify searches and seizures in a wide variety of situations where an officer is instructed to undertake the search but is not provided information sufficient to independently find the proper level of individualized suspicion.

The rationale behind the collective knowledge rule is largely pragmatic: “‘[E]ffective law enforcement cannot be conducted unless police officers can act on directions and information transmitted by one officer to another and … officers … cannot be expected to cross-examine their fellow officers about the foundation for transmitted information.’” Requiring that the officer who engages in a search or seizure must herself have the necessary individualized suspicion would be a “crippling restriction[] on our law enforcement.” Instead, it is sufficient that at some point an individual trained in making individualized suspicion determinations, be she a magistrate or a law enforcement officer, had sufficient knowledge to conclude that the individual be seized or searched. Requiring that a person trained in individualized suspicion determinations find probable cause or reasonable suspicion seems to ensure that reliance on the instruction to stop is objectively reasonable. In addition, an individual

---

142 United States v. Williams, 627 F.3d 247, 252 (7th Cir. 2010).
143 Hensley, 469 U.S. at 232. The search or seizure also must not exceed the scope justified by the underlying individualized suspicion. Williams, 627 F.3d at 252.
144 For a thorough discussion of the various permutations of the collective knowledge rule, see Stern, supra note 37, at 1094–1105.
145 Hensley, 469 U.S. at 231 (quoting United States v. Robinson, 536 F.2d 1298, 1299 (9th Cir. 1976).
146 United States v. Lyons, 687 F.3d 754, 766 (6th Cir. 2012).
147 See United States v. Colon, 250 F.3d 130, 135 (2d Cir. 2001) (“A primary focus in the imputed knowledge cases is whether the law enforcement officers initiating the search or arrest, on whose instructions or information the actual searching or arresting officers relied, had information that would provide reasonable suspicion or probable cause to search or arrest the suspect.”).
148 See Colon, 250 F.3d at 138 (finding that police officer reliance on information known to 911 operator was objectively unreasonable because operator was not training in making individualized suspicion determinations).
searched or seized pursuant to the collective knowledge doctrine has “minimal” interests at stake.\textsuperscript{149} Because the suspect could have been seized by one officer, she loses little in the way of security or privacy when she is stopped by another at the instruction of the first.\textsuperscript{150}

While the constructive knowledge doctrine applies the general idea underlying the collective knowledge doctrine of police reliance on other officers’ knowledge, it does so without the same strict requirements.\textsuperscript{151} The broadest view of the constructive knowledge doctrine, and the one most relevant here, is found in which no one officer possesses facts sufficient to establish the needed individualized suspicion, but the aggregation of several officers’ knowledge would meet the standard.\textsuperscript{152} Specifically, this version of the doctrine omits both the requirement that a single individual trained in individualized suspicion assessments evaluate the facts and the need for the officers whose knowledge will be collected to have communicated with each other.\textsuperscript{153} Nevertheless, courts generally limit the scope of the constructive knowledge doctrine to officers who are working closely together.\textsuperscript{154}

Academics and dissenting judges have criticized the constructive knowledge doctrine on the ground that it does not meaningfully enhance law enforcement expediency, because police communication is cheap and increases accuracy.\textsuperscript{155} Moreover, the constructive knowledge doctrine removes the concept of “belief” and the perspective of a “reasonable officer” from the definitions of probable cause and reasonable suspicion.\textsuperscript{156} After all, a court cannot inquire into whether “facts and circumstances within the officer’s knowledge [] are sufficient to warrant a prudent person, or one of reasonable caution, in believing” that the suspect is engaged in criminal conduct if no single officer knew the

\begin{itemize}
\item \textsuperscript{149} Hensley, 469 U.S. at 682.
\item \textsuperscript{150} Stern, supra note 37, at 1090.
\item \textsuperscript{151} Id. at 1105.
\item \textsuperscript{152} See id. at 1106–9 & nn.80–101 (discussing cases).
\item \textsuperscript{153} Id. at 1109.
\item \textsuperscript{154} Id. at 1108–9.
\item \textsuperscript{155} Id. at 1111 & n.107.
\item \textsuperscript{156} Id. at 1112–13.
\item \textsuperscript{157} Michigan v. DeFillippo, 443 U.S. 31, 37 (1979).
\end{itemize}
information and could believe something about it. Finally, as massive quantities of information become readily available to law enforcement agencies through fusion centers and communication technologies, a broad reading of the constructive knowledge doctrine would render the individualized suspicion requirement meaningless in most situations. This threat has led one scholar to suggest that the constructive knowledge doctrine would turn the police into “something like Star Trek’s Borg Collective,” in that officers will be able to rely upon what is known by any other officer anywhere, at least for the purposes of providing a post hoc justification for a search or seizure.

B. Applying the Doctrines to ASAs

The power of ASAs to analyze large quantities of data in making their predictions underscores the threat that the constructive knowledge doctrine poses to the Fourth Amendment’s individualized suspicion requirement. Where police have access to the massive troves of information contained in fusion centers, the doctrine already opens the door to “arrest-first-justify-later” policing. But permitting police to claim constructive awareness of an ASAs’ predictions of criminality without any requirement that the prediction be communicated to officer conducting a search or seizure would further encourage police to ignore individualized suspicion

---

158 See Citron & Pasquale, supra note 6, at 1448–55 (discussing the role of fusion centers in collecting and distributing information to law enforcement agencies).
159 See Poniatowski, supra note 37, at 842 (“The communication/network requirement of the constructive-knowledge doctrine has been applied leniently by some courts, threatening to eviscerate the [probable cause] requirement altogether.”) (internal citations omitted).
160 Stern, supra note 37, at 1114.
161 Of course, there are those who argue that the individualized suspicion requirement fails to advance the interests underlying the Fourth Amendment in some situations and should be replaced. See, e.g., Bernard E. Harcourt & Tracey L. Meares, Randomization and the Fourth Amendment, THE U. OF CHI. L. REV. 809, 816 (2011) (contending that “individualized suspicion” should be abandoned in favor of randomized searches). These proposals may have merit, but the constructive knowledge doctrine threatens an even more dismal state of affairs than what currently exists, as the individualized suspicion doctrine would survive, but without what few teeth it has now.
162 Poniatowski, supra note 37, at 851.
requirements. Particularly as criminal laws have proliferated to the point that “everyone is a criminal if prosecutors look hard enough,”\textsuperscript{163} applying the constructive knowledge doctrine to ASAs could permit the police to stop anyone and later find a prediction of crime to justify the intrusion.

Applying the collective knowledge doctrine to ASAs presents a less immediately discomfiting dystopia. Upon receipt of an ASA’s prediction, police could search or seize a person identified by an ASA without engaging in any independent assessment of the facts to determine whether individualized suspicion exists. Reliance by the police officer would be permitted if the ASA’s prediction is analogous to an instruction to arrest by an individual trained in making individualized suspicion determinations.\textsuperscript{164} In some sense, an ASA seems very well-trained in making individualized suspicion determinations, as it can provide a quantifiable prediction of criminality based on the available data, \textit{e.g.}, there is a 60\% chance that the person on a certain street corner is dealing drugs.\textsuperscript{165} So long as we have reason to believe that the ASA is accurate,\textsuperscript{166} the ASA’s prediction is arguably analogous to an assertion of the existence of probable cause or reasonable suspicion by a person trained in making such assessments. The Court, after all, has repeatedly explained that individualized suspicion deals with probabilities,\textsuperscript{167} and an ASA can quantify those probabilities like no technologies before it.

This analogy between an ASA and a trained person fails for two related reasons, however. First, the analogy depends on a fundamental misunderstanding of the question that the individualized suspicion standard asks. Second, the analogy fails to appreciate differences in how humans and machines examine factual situations. To see these flaws, we

\textsuperscript{164} \textit{See supra} note 147 and accompanying text.
\textsuperscript{165} When a machine learning algorithm generates an association rule from data – \textit{i.e.}, it predicts that when certain antecedent conditions are satisfied, some consequent condition will also exist – confidence measures the accuracy of the rule when the antecedent conditions are satisfied. KONONENKO \& MATJAZ, \textit{supra} note 14, at 233–34.
\textsuperscript{166} The factors that go into determining the accuracy of an ASA are discussed \textit{infra} § IV.C.
must start by recalling the probable cause and reasonable suspicion determinations require a consideration of the totality of the circumstances. As its name suggests, the totality-of-the-circumstances approach demands a consideration of all evidence relevant to the question of how likely it is that the targeted individual is engaged in criminal activity, including exculpatory evidence.

For an ASA’s prediction to be sufficient to justify a search or seizure, it too must engage in a totality-of-the-circumstances analysis. But, at least under current technological constraints, ASAs are fundamentally incapable of doing so. As with any machine learning process, an ASA is only as good as the data its programmers choose to provide it, either in training or in real-world application. This is because the data provided to an ASA constitutes the sum total of what the algorithm “knows” about the world; the ASA cannot identify new types of relevant data that are not currently contained in its dataset and seek out those data. Thus, an ASA trained on a small dataset “knows” very little about, while an ASA trained on an enormously robust dataset “knows” quite a lot. But even the latter ASA is limited in making its predictions to analysis of the data within its dataset, and it cannot consider other facts that might be relevant.

This limitation is in contrast to the capacities of human beings, who are always at least potentially capable of including a new piece of relevant information in an analysis. And this distinction matters enormously for

---

169 See supra note 99 and accompanying text.
170 See notes 73-78 and accompanying text; Surden, supra note 44, at 106 (“In general, machine learning algorithms are only as good as the data that they are given to analyze.”).
171 While “active learning,” where a machine learning algorithm chooses the data with which to be trained, is a goal of a sub-field of machine learning research, even an active learning algorithm is limited to considering the data provided to it. See Burr Settles, Active Learning Literature Survey, Computer Sciences Technical Report 1648, University of Wisconsin-Madison 4 (2009), available at http://www.active-learning.net.
172 This is not to say that humans do not suffer from cognitive biases that may substantially undermine their ability to make accurate individualized suspicion determinations. See Christopher Slobogin, Why Liberals Should Chuck the
the capacity of an ASA to engage in a totality-of-the-circumstances analysis. The kinds of information that might be relevant to an individualized suspicion determination are almost infinitely diverse. Thus, while an ASA may be trained with a database that contains all the facts that are most relevant in a large majority of cases, that database cannot contain all the facts that are relevant in all the cases. As a result, an ASA cannot, as required by the Fourth Amendment, consider the “whole picture” regarding a person’s potentially criminality.

To illustrate this point, imagine a baseball team that trains a machine learning algorithm to predict which players will be most effective offensively and defensively for each upcoming game. The team provides the algorithm with all available historical game data about player performance. Through the training process, the algorithm would learn to consider whatever information in that database correlates to each individual player’s performance. On the morning of a particularly important game, the algorithm reports to Manager that Sub should be given the start over Star. Shortly before submitting his roster for the game, Manager sees Sub in the locker room reeking of alcohol and appearing extremely hungover. Certainly, it seems logical that being hungover would impact Sub’s performance in the game and therefore should impact Manager’s decision of which player to start. But data about Sub’s alcohol consumption the night before, and his feelings of being hungover on game-day, were not captured in the otherwise-robust dataset

---

173 This observation can be confirmed by any Criminal Procedure professor who has had a student fond of imagining their own hypotheticals.

174 Another limitation on an ASA’s capacity to consider all potentially relevant facts is that a machine learning algorithm can consider only “features” that are quantifiable. See supra note 54 and accompanying text.


176 The frequency of games and enormity of the resulting datasets has made baseball a prime area for statistical analysis generally, and a tempting target for machine learning applications. See, e.g., Randy Jia et al., Predicting the Major League Baseball Season (Autumn 2013) (on file with the author) (using machine learning approaches to predict the outcome of games in the 2012 Major League Baseball season).
provided to the algorithm. Therefore, the algorithm, though not flawed, has not analyzed the totality of the circumstances relevant to player performance. Of course, now that Manager has identified a new type of relevant information, data of that sort may now be included in the dataset used to continuously train the algorithm. But we can continue to imagine more pieces of information that are missing: drug consumption, either performance-enhancing or otherwise, marital problems, injuries, other personal issues, etc. And though the algorithm may be constantly improved, the dataset on which it is trained can never fully encapsulate all facts potentially relevant to player performance.

Similarly, a police officer or magistrate may already know or may learn prior to the search or seizure a piece of information that is not captured in the ASA’s dataset, but which is relevant to predicting whether a suspect is engaged in criminal conduct. The totality of the circumstances analysis requires that this information be factored into the probable cause or reasonable suspicion determination. And because human beings are capable of considering this additional data on the fly, only a human being can undertake a totality of the circumstances analysis that satisfies the Fourth Amendment. Of course, as with the baseball example, if the new information is of a type that can be quantified and collected, it can be added to the dataset, and the ASA can refine its predictions. The potential for refinement, however, does not satisfy the Fourth Amendment, and the facts that may be relevant to the individualized suspicion question in

---

177 The human capacity to be open to consideration of new relevant data is related to what Orin Kerr has called "instinct" or "intuition" in arguing against the quantification of individualized suspicion standards. See Orin Kerr, Why Courts Should Not Quantify Probable Cause, in THE POLITICAL HEART OF CRIMINAL PROCEDURE: ESSAYS ON THEMES OF WILLIAM J. STUNITZ 131, 138 (Michael Klarman et al. eds., 2012). Kerr’s “instinct” involves the recognition that sometimes there is important information missing from the facts currently available in an individualized suspicion analysis. The missing data may be inculpatory, exculpatory, or relevant from a policy standpoint. See id. at 138-39 (noting that the desired evidence may tie the suspect more closely to the crime or its absence may suggest something important about police motives). Courts have typically resisted imposing any duty on police officers to investigate further once known facts are sufficient to establish individualized suspicion, however. Thus, the fact that machine learning algorithms lack what Kerr calls "instinct" does not provide an independent reason why ASAs cannot undertake a totality of the circumstances analysis.
every situation are so multifarious that no dataset could realistically capture them all. Thus, a person trained in making individualized suspicion determinations must be the final assessor of the totality of the circumstances, including both the ASA’s prediction and any other relevant available data, and decide whether the probable cause or reasonable suspicion standards are met.\footnote{While the Fourth Amendment requires a consideration of all known facts, it does not impose a duty to investigate on police once individualized suspicion has been established. \textit{See} Ahlers v. Schebil, 188 F.3d 365, 371 (6th Cir. 1999) (“Once probable cause is established, an officer is under no duty to investigate further or to look for additional evidence which may exculpate the accused.”). Thus, the obligation of police to consider the totality of the circumstances is phrased in terms only of \textit{available} data.}

It must be recognized, however, that requiring a human to assess the totality of the circumstances may reduce the overall accuracy of police searches and seizures. While some of the additional evidence that a human being will consider may be clear-cut in confirming or rebutting the ASA’s prediction, the impact of other evidence on the analysis is likely to be less clear. For instance, imagine that an ASA predicts that a specific individual, who has been going from car-to-car in a parking lot before spending five minutes trying to get into one vehicle before walking away, has a 52% chance of being engaged in auto theft. If the ASA is believed to be accurate, these odds almost certainly would be enough to establish probable cause to arrest the suspect.\footnote{\textit{See} Craig S. Lerner, \textit{The Reasonableness of Probable Cause}, 81 \textit{Texas L. Rev.} 951, 996 (2003).} An officer is told of the ASA’s prediction and approaches the individual near the parking lot. The officer, it turns out, knows the individual personally and asks him for an explanation. The individual provides a story that innocently explains his actions. If the officer finds the story credible, that fact would destroy the officer’s probable cause. Thus, considering the totality of all the circumstances known to him, the officer could not validly arrest the suspect.

Yet, there are serious reasons to doubt the officer’s ability to accurately assess a suspect’s credibility.\footnote{\textit{See} Andrew E. Taslitz, \textit{Neuroscience, Cognitive Psychology, and the Criminal Justice System}, 8 \textit{Ohio St. J. Crim. L.} 7, 27–29 (2010) (collecting research); Eugenio Garrido} Thus, there are good reasons to think that
the officer’s independent totality-of-the-circumstances analysis is less likely to accurately predict whether the suspect is engaged in criminal conduct than the ASA’s original prediction. Indeed, police face numerous cognitive roadblocks in making accurate individualized suspicion determinations. In additional to their troubles with credibility determinations, irrelevant facts, like a suspect’s race, religion, or national origin, may influence the officer’s assessment of criminality. Finally, incorporating the output of an ASA in the totality-of-the-circumstances analysis in an accurate and meaningful way is likely to be quite challenging. Consequently, requiring police to be open to additional data and include such data in their totality-of-the-circumstances analysis for each suspect will likely lead to more police errors: namely, searches and seizures of the innocent and instances of the guilty going free.

This result is certainly not ideal, but the Fourth Amendment and its individualized suspicion standards are not in place to maximize police accuracy; rather, they aim to ensure individualized justice. In other words, the Fourth Amendment would not be satisfied if a police agency conducted ten searches, five on suspects who were almost certainly engaged in criminal activity and five on suspects who almost certainly were not, on the ground that on average probable cause existed. Rather, probable cause must exist for each suspect. In other words, the Fourth

---

181 See Taslitz, supra note 180.
182 See L. Song Richardson, Arrest Efficiency and the Fourth Amendment, 95 MINN. L. REV. 2035, 2045–48 (2010) (collecting research showing the impact of implicit bias on police evaluation of situations).
183 See infra § IV.
185 The Fourth Amendment is sometimes interpreted by the Court in a manner consistent with it being a collective, rather than an individual, right. See Thomas K. Clancy, Fourth Amendment as a Collective Right, The, 43 TEX. TECH L. REV. 255, 263–94 (2010). Nonetheless, this interpretation is generally limited to situations outside of police interdiction of ordinary criminal activity. See Id. at 273–90 (discussing examples of situations where the Fourth Amendment is viewed as a collective right).
Amendment requires in most circumstances that each suspect is entitled to an assessment of whether individualized suspicion exists based on all available facts relating to her potential guilt.\textsuperscript{186} Recent approaches to probable cause and reasonable suspicion may have undermined the individualized nature of these standards,\textsuperscript{187} but the requirement of a totality of the circumstances analysis remains, even if that requirement means that police will make more mistakes.

IV. ASAs AS PART OF THE TOTALITY OF THE CIRCUMSTANCES

If an ASA’s output alone cannot satisfy the individualized suspicion requirements of the Fourth Amendment, it must be considered as a part of the totality-of-the-circumstances analysis. As explained above, ASAs are unique data sources in that they aim to assist in the second step of the individualized suspicion analysis by providing information about when one should infer criminality from certain historical facts.\textsuperscript{188} Though they can be the source of bad law, when it comes to new technologies and the Fourth Amendment, analogies to existing data sources are the currency of the realm.\textsuperscript{189} A good analogy should help courts and police identify the factors that will help them separate reliable ASAs from unreliable ones. This section will explore three potential analogies. First, ASAs bear similarity to police profiles, such as those frequently used to identify drug

\textsuperscript{186} As Taslitz correctly notes, the fact that there are exceptions to the individualized suspicion requirement does not mean that the Fourth Amendment’s commitment to individualized justice is any less important. See Andrew E. Taslitz, Search and Seizure History as Conversation: A Reply to Bruce P. Smith, 6 OHIO ST. J. CRIM. L. 765, 775 (2009).

\textsuperscript{187} See generally David A. Harris, Particularized Suspicion, Categorical Judgments: Supreme Court Rhetoric Versus Lower Court Reality under Terry v. Ohio, 72 ST. JOHN’S L. REV. 975 (1998) (critiquing how lower courts have permitted categorical judgments to satisfy the Fourth Amendment’s individualized suspicion standards).

\textsuperscript{188} See supra § II.B.

\textsuperscript{189} Though analogies are often the source of bad law, they are the currency of the realm when courts deal with new technologies. See Kerr, supra note 36, at 875–76 ("Judges struggle to understand even the basic facts of [new] technologies, and often must rely on the crutch of questionable metaphors to aid their comprehension. Judges typically will not know whether these metaphors are accurate...."),
couriers, human traffickers, child abusers, or terrorists, as they utilize historical information to identify traits that are commonly held by criminals with the goal of predicting future criminality. Second, algorithms are akin to informants in that people outside of law enforcement are providing information to police, albeit indirectly through the ASA. Third, algorithms are similar to drug-sniffing dogs in that both resemble “black boxes” that create outputs from known inputs and potentially uncertain processes. This section addresses each potential analogy in turn. The first two analogies are ultimately unhelpful for substantive and procedural reasons. The third is more useful, though it is also imperfect. This section concludes by identifying lingering challenges in how to incorporate ASAs into the totality-of-the-circumstances analysis.

A. Algorithms as Police Profiles

Traditional police profiles are “abstract[s] of characteristics thought typical of persons” engaged in certain criminal activity. These characteristics often include traits or behavior that are legal and innocent when considered alone, but become suspicious in a given context or when considered conjunctively. For instance, in United v. Sokolow, the profile of a drug courier on an airplane included innocent facts like: (1) paying for plane tickets in cash; (2) traveling under a name that does not

---

191 See Ferguson, supra note 16, at 308–10 (comparing “predictive policing” technologies, which predict where crime is likely to occur, to a police profile).
192 See Id. at 305–8 (comparing predictive policing to an informant’s tip); see also Elizabeth E. Joh, Policing by Numbers: Big Data and the Fourth Amendment, 89 WASH. L. REV. 35, 56-57 (2014) (expanding somewhat on Ferguson’s analysis).
193 See Goldberg, supra note 40, at 791 n.9 (noting the similarity between drug dogs and “other machines used by police or forensic scientists).
195 See United States v. Sokolow, 490 U.S. 1, 9 (1989) (where DEA agents stopped defendant who fit drug courier profile, stop is valid even though each individual factor was “consistent with innocent travel,” because “taken together they amount to reasonable suspicion”).
196 Id.
match the name listed with one’s phone number; (3) traveling from a “source city” for drugs; (4) staying in the source city for a brief period, particularly when compared to the length of the flight to get there; (5) appearing nervous; and (6) not checking luggage. Profiles like this one formalize the traditional policing process of examining an individual’s non-criminal characteristics and actions to determine whether, when taken together, they create suspicion of criminal conduct. Taken in their best light, profiles consolidate and perpetuate the experience of numerous officers, thus allowing even junior officers to be smart at detecting crime, much in the way that police training instills the experience of veterans in new recruits.

Though somewhat confusing, the Supreme Court’s guidance on profiles suggests that they matter, but only indirectly, to the individualized suspicion analysis. First, the Court has been clear in saying that a profile qua profile does not justify an inference of individualized suspicion. In other words, a set of facts should receive neither any greater nor any lesser weight because those facts are contained in something that a certain law enforcement agency has called a profile of criminal activity. Rather, a reviewing court must look de novo at a police officer’s determination that the facts contained in a police profile support the necessary individualized inference of suspicion.

---

197 See id. at 1.
198 See id. at 9-10 (“Indeed, Terry itself involved ‘a series of acts, each of them perhaps innocent’ if viewed separately, ‘but which taken together warranted further investigation.’”) (quoting Terry v. Ohio, 392 U.S. 1, 22 (1968)); Milton Heumann & Lance Cassak, Profiles in Justice-Police Discretion, Symbolic Assailants, and Stereotyping, 53 RUTGERS L. REV. 911, 918 (2000) (“profiling often comes to focus on behavior that is perfectly legal and in other contexts (perhaps even in the context at hand) purely innocent”).
200 See Sokolow, 490 U.S. at 10 (“We do not agree with respondent that our analysis is somehow changed by the agents’ belief that his behavior was consistent with one of the DEA’s ‘drug courier profiles.’”).
201 See Ornelas v. United States, 517 U.S. 690, 699 (1996) (“We hold therefore that as a general matter determinations of reasonable suspicion and probable cause should be reviewed de novo on appeal.”); see, e.g., Sokolow, 490 U.S. at 9-10 (finding
distillation of police experience that certain facts, when found in conjunction, are indicative of criminal conduct, that experience is entitled to some deference. 202

Requiring courts to engage in de novo reviews of traditional profiles makes sense. 203 We expect police to examine the facts in an individual case and use typical tools of reason and logic—induction, deduction, and the like—to decide whether they suggest the existence of criminal activity. Yet police are engaged in the “often competitive enterprise of ferreting out reasonable suspicion through independent analysis of facts contained in drug courier profile); United States v. Montoya de Hernandez, 473 U.S. 531, 541-42 (finding reasonable suspicion based on review of all facts where defendant stopped by customs agent using a drug courier profile); Reid v. Georgia, 448 U.S. 438, 440-41 (1980) (finding that facts that “appeared to the agent to fit the so-called ‘drug courier profile’” were insufficient to create reasonable suspicion) (per curium). 202 See Ornelas v. United States, 517 U.S. 690, 699 (1996) (recognizing that when “a police officer views the facts through the lens of his police experience and expertise,” the inferences he draws “deserve deference”); United States v. Mendenhall, 446 U.S. 544, 564 (1980) (Powell, J., concurring) (noting, where suspect allegedly fit DEA profile, that “in all situations the officer is entitled to assess the facts in light of his experience”) (quoting United States v. Brignoni-Ponce, 422 U.S. 873, 885 (1975)). 203 It bears mention that this approach is effective only when lower courts engage in the analysis with the appropriate balance of deference and skepticism toward police decisions, and experience shows that courts may have difficulty striking that balance. See David Cole, Discretion and Discrimination Reconsidered, 87 Geo. LJ 1059, 1077-79 (1998) (providing catalogue of facts cited by courts as factors in DEA drug courier profiles and concluding that “[s]uch a profile does not meaningfully narrow the field of potential suspects”); see also Sharon L. Davies, Profiling Terror, 1 Ohio St. J. Crim. L. 45, 60-61 (2003) (“Despite scholarly criticism, courts tended to uphold reliance on drug courier profiles prior to September 11 provided law enforcement agents who relied on those profiles did not consider an individual’s race or ethnicity in isolation in calculating reasonable suspicion.”); Charles L. Becton, The Drug Courier Profile: ‘All Seems Infected That th’ Infected Spy, As All Looks Yellow to the Jaundic’d Eye’, 65 N.C. L. Rev. 417, 469 (1987) (“[L]ower courts have sanctioned profile stops with increasing regularity.”). Similarly, courts must engage in a meaningful inquiry into an officer’s training and experience to be able to properly assess its impact on the individualized suspicion analysis. Unfortunately, there is ample evidence that many courts fail to engage in such an inquiry. See Richardson, supra note 117, at 1158–60. These concerns suggest there are serious issues with how the Court’s approach has been implemented, but do not undercut its logic.
Thus, police have some incentive to push boundaries, which in this case might mean constructing a “chameleon-like” profile that can fit any situation. A judge, on the other hand, should have no skin in the game. Thus, when presented with the same facts that were available to the police at the time, including background on the relevant officer’s training and experience, she can double-check the officer’s logic dispassionately. This process ideally ensures that the police reasoned logically and reached a defensible conclusion that the facts supported a sufficient inference of criminal suspicion. Similarly, the court can ensure that enough facts exist regarding the specific target of the search or seizure to support a finding of suspicion that is sufficiently individualized.

On the surface, then, an ASA is like a police profile, in that it identifies likely criminals through the coexistence of multiple innocent facts gleaned from past experience. But substantial differences lie beneath this superficial analogy. First, ASAs derive their conclusions from hard data. In order to “learn” a correlation between certain conduct or characteristics and criminal activity, an ASA must process training data derived from real-life situations. Traditional profiles, on the other hand, are frequently criticized for the absence of data showing that a person meeting the profile is likely engaged in criminal conduct. Similarly, ASAs, like

---

205 Sokolow, 490 U.S. at 13-14 (Marshall, J., dissenting); see also United States v. Hooper, 935 F.2d 484, 499-500 (Pratt, J., dissenting) (listing contradictory characteristics that have been claimed to be part of drug courier profiles).
206 See Johnson, 333 U.S. at 14 (noting that the Fourth Amendment requires assessment of the facts by a “neutral and detached magistrate”).
208 See Morgan Cloud, Search and Seizure by the Numbers: The Drug Courier Profile and Judicial Review of Investigative Formulas, 65 B.U.L. REV. 843, 920 (1985) (concluding that mechanical application of drug courier profiles violates the Fourth Amendment’s requirement of individualized suspicion).
209 See supra notes 61-64 and accompanying text. As will be discussed shortly, this reliance on hard data makes ensuring the quality of the underlying data even more important. See infra § IV.D.
210 See Heumann & Cassak, supra note 198, at 918 (“Less precise than arrest-based historical data, but also frequently mentioned as a basis for identification of
other machine learning algorithms, can examine exponentially more data points about a person or situation than could reasonably be listed in a traditional profile.\textsuperscript{211}

Second, ASAs can identify more complex relationships between observable data and criminal activity than the simple checklist of a traditional profile, which is often applied without clear standards.\textsuperscript{212} Even an ASA that applies basic machine learning algorithms can check not only for the existence of particular facts, but it can also assign a weight to each fact depending on the strength of its correlation to criminal activity.\textsuperscript{213} Likewise, an ASA can assess the interdependency of variables, \textit{i.e.}, the extent to which the occurrence of criminal activity depends not just on the existence of single variable, but on the concurrent existence or non-existence of multiple variables.\textsuperscript{214} For example, thinking back to the facts in the profile in \textit{Sokolow}, an ASA might reveal that paying for a ticket in cash and not checking a bag do not, each standing alone, predict drug trafficking with any particular strength, but that the concurrence of the two factors is highly predictive. An ASA’s capacity for examining a multitude of variables and to identify complex relationships amongst them means, however, that the rules generated by an ASA may not be interpretable even to the ASA’s programmers.\textsuperscript{215}

\textsuperscript{211} For example, an e-mail spam filter may have a vocabulary of 10,000 terms that it uses to predict whether a given e-mail is spam. \textit{Flach}, supra note 10, at 9.

\textsuperscript{212} Traditional profiles are often informal, unwritten, and do not state how many of a set list of factors must be met before the profile is satisfied. Heumann & Cassak, supra note 198, at 919–21.

\textsuperscript{213} \textit{Flach}, supra note 10, at 25–32 (discussing the use of probability functions to determine the likelihood of an event occurring depending the existence of each variable).

\textsuperscript{214} \textit{See id.} at 44 (“One fascinating and multi-faceted aspect of features is that they may interact in various ways. Sometimes such interaction can be exploited, sometimes it can be ignored, and sometimes it poses a challenge.”).

\textsuperscript{215} \textit{See supra} notes 88–91 and accompanying text.
The differences between traditional profiles and ASAs make the Supreme Court’s approach to traditional profiles unhelpful and counterproductive when applied to ASAs. First off, unless an ASA is interpretable, no one will be able to explain to a reviewing court how or why the algorithm made its prediction. Thus, the court simply will be unable to double-check the ASA’s work. Alternatively, an ASA could be programmed to be interpretable.\(^{216}\) Even then, the “logic” of an ASA is not of the sort that a judge can easily double-check. One benefit of an ASA is its capacity to identify correlations within data that are not obvious, but which are statistically valid.\(^{217}\) In other words, an ASA could identify a set of behaviors that correlate strongly to criminal conduct, even though the logical connection between the behavior and criminality—i.e., why a criminal would engage in that behavior—is unclear. The absence of a clear logical connection does not mean that the behavior is a bad predictor of criminality; rather, the logic of the correlation may be surprising, or the available dataset may fail to contain the information needed to understand it.\(^{218}\) Yet a court treating the ASA like a traditional profile, and needing a logical explanation for why certain facts predict criminality, would reject the ASA’s prediction, no matter the level of confidence the ASA has in the prediction.

In sum, courts treating ASAs like police profiles may demand that the ASAs be interpretable, thus undermining their effectiveness,\(^ {219}\) and may reject accurate predictions as “illogical.” At the same time, the profile analysis would ignore the real sources of ASA inaccuracy, which typically

\(^{216}\) The issue of whether the interpretability of ASAs should be mandated involves a number of policy questions that are outside the scope of this Article. See Zarsky, supra note 34, at 1526–30.

\(^{217}\) See Colonna, supra note 43, at 313 (relating a “canonical anecdote” about a supermarket that used data mining to discover a correlation between purchases of diapers and beer as “an example of unpredictable knowledge found in a huge dataset”); Surden, supra note 44, at 107 (“Machine learning techniques are also useful for discovering hidden relationships in existing data that may otherwise be difficult to detect.”).

\(^{218}\) See, e.g., Surden, supra note 44, at 108–9 (suggesting that machine learning may allow analysis of court opinion to unearth unarticulated bases for judicial decisions).

\(^{219}\) See supra note 91 and accompanying text.
occur in the training and programming of the algorithm.\textsuperscript{220} Consequently, courts should look elsewhere to find useful analogies for ASAs.

B. Algorithms as Informants

An informant is, under the most general definition, a non-police-officer who provides information to the police.\textsuperscript{221} Traditional informants include jailhouse snitches, criminal accomplices, concerned citizens, and innocent eyewitnesses.\textsuperscript{222} Little ties informants together beyond the fact that they are civilians, not trained law enforcement agents. As a result, their information does not fall within the scope of the Fourth Amendment’s collective knowledge doctrine.\textsuperscript{223} For analytical purposes, informants can be subdivided into three categories: (1) criminal informants; (2) anonymous tipsters; and (3) citizen-informants.\textsuperscript{224} ASAs are clearly not analogous to criminal informants, who provide police with information about their own criminal contacts in exchange for money or leniency.\textsuperscript{225} Rather, as will be explained, ASAs share characteristics of both anonymous tipsters and citizen-informants. The former, as evident from their name, are individuals who provide information to the police, but whose identity is not known. The latter are known civilians who provide police with information that they happen to have obtained out of the bad luck of being the victim or witness of a crime.\textsuperscript{226}

When assessing the weight to be given to a tip in the individualized suspicion analysis, courts look to whatever is known about the informant’s

\textsuperscript{220} See supra notes 69-87 and accompanying text.

\textsuperscript{221} Michael L. Rich, Coerced Informants and Thirteenth Amendment Limitations on the Police-Informant Relationship, 50 SANTA CLARA L. REV 681, 689 (2010).

\textsuperscript{222} Id. at 689–90.

\textsuperscript{223} See notes 147-148 and accompanying text; see also United States v. Ventresca, 380 U.S. 102, 111 (1965) (“Observations of fellow officers of the Government engaged in a common investigation are plainly a reliable basis for a warrant applied for by one of their number.”).


\textsuperscript{225} Id. at 2343–44.

\textsuperscript{226} Id. at 2341.
veracity and reliability. To assess the tipster’s veracity, courts will look to relevant data like her purported motivations for helping the police, her previous history of providing accurate information, and her reputation in the community. The reliability of a tip traditionally depends on whether the tip is based on personal knowledge or is so detailed that it is likely to have come from someone with first-hand information. In addition, police corroboration of a tip’s details enhances the reliability of the tip substantially, with corroboration of predictions about future conduct being particularly valuable.

Courts treat anonymous tips and tips by citizen-informants very differently. Because the source of an anonymous tip is, by definition, unknown to the police, an anonymous tip provides “virtually nothing” to suggest the tipster’s honesty and gives “absolutely no indication” of the basis for the tipster’s information. Moreover, anonymous tipsters are not to be trusted because, unlike known informants, they cannot be held responsible for fabricated allegations. As such, an anonymous tip generally must be corroborated before it can be assigned much weight in the individualized suspicion. Specifically, corroboration of an

---

229 See United States v. Bush, 647 F.2d 357, 362 (3d Cir. 1981) (noting that a track record of accurate tips is “the typical basis for a finding of veracity”).
231 See, e.g., United States v. Nieman, 520 F.3d 834, 840 (8th Cir. 2008) (relying on the first-hand nature of informants’ information to sustain finding of probable cause).
233 Id. at 245.
234 Id. at 227.
236 See Gates, 462 U.S. at 227 ("The Illinois Supreme Court concluded—and we are inclined to agree—that, standing alone, the anonymous letter … would not provide the basis for a magistrate’s determination that there was probable cause to believe contraband would be found …").
anonymous tip’s predictions about future conduct provides the most weight in establishing the tipster’s credibility and basis of knowledge.\textsuperscript{237}

Tips from citizen-informants, on the other hand, are generally accorded great weight. Many courts adhere to the “citizen-informant doctrine,” by which information provided by “regular” or “ordinary” citizens can be relied upon in the individualized suspicion analysis without corroboration.\textsuperscript{238} In particular, courts are willing to trust non-criminal informants because they have no (apparent) reason to lie and they can be punished if they falsely report a crime.\textsuperscript{239}

ASAs fit the broad definition of informants, in that they are outside of law enforcement and provide information to police about criminal activity, but they are not neatly characterized as either anonymous tipsters or citizen-informants.\textsuperscript{240} With respect to veracity, it is immediately obvious that ASAs are not people with personalities, codes of morality, motivations, or the capacity for honesty and dishonesty.\textsuperscript{241} As such, discussion of an ASA’s veracity is nonsensical. But ASAs are programmed by people, and an ASA will inevitably reflect the conscious and unconscious biases and motivations of its programmers.\textsuperscript{242} Such biases and motivations are generally irrelevant to the individualized suspicion analysis, however, unless they provide a reason for the police to doubt the underlying

\textsuperscript{237} J.L., 529 U.S. at 272.

\textsuperscript{238} Werner, supra note 224, at 2339.

\textsuperscript{239} Id. at 2360.

\textsuperscript{240} See Ferguson, supra note 16, at 305–10 (attempting, with limited success, to analogize “predictive policing algorithms” that identify where crime is likely to occur to an informant’s tip).

\textsuperscript{241} See Id. at 307 (“The computer has no biases, no past bad acts, and no agendas.”). This is not to say that something meant to replicate human personality, morality, or honesty could not be programmed into an automated process. See, e.g., George R. Lucas, Jr., Automated Warfare, 25 STAN. L. & POL’Y REV. 317 (2014) (arguing that we could achieve “robot morality” by programming unmanned vehicles to follow the moral and legal demands of war as well or better than human beings). An ASA is unlikely to involve such programming, however, given its limited purpose.

\textsuperscript{242} See Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 WASH. L. REV. 1, 4 (2014) (“Because human beings program predictive algorithms, their biases and values are embedded in the software's instructions...”).
accuracy of the information.\textsuperscript{243} It stands to reason, though, that a police department would be displeased with an ASA if courts found reliance on the ASA’s predictions to be objectively unreasonable and excluded evidence obtained as the result of such reliance.\textsuperscript{244} An ASA’s programmers therefore have a financial incentive, albeit a somewhat attenuated one, to provide an ASA that is reliable enough for the police to rely upon it in finding individualized suspicion. Such an incentive may not compel accuracy as strongly as the threat of prosecution to a citizen-informant, but it does provide some reason to believe that an ASA is “credible.”\textsuperscript{245}

Looking to the motivations of an ASA’s programmers to assess how much weight to put on an ASA’s prediction is odd, however, given that data should be available about an ASA’s proven or anticipated reliability. As noted, an ASA’s prediction should come with a confidence level that can provide a tangible measure of the ASA’s potential predictive power.\textsuperscript{246} Moreover, data can be collected about the performance of the ASA that can then be used to establish its reliability.\textsuperscript{247} This sort of data does have a place in the Court’s informant analysis, in that tips from informants who have proven to be reliable in the past are given greater weight.\textsuperscript{248} But the

\textsuperscript{243} See U.S. v. Perez, 651 F.2d 268 (5th Cir. 1981) (“The motives upon which informants act in reporting crimes are generally irrelevant....”); cf. Whren v. United States, 517 U.S. 806, 813 (1996) (holding that the subjective intentions of the police typically play no role in the probable cause analysis).


\textsuperscript{245} On this point, I differ with Andrew David Ferguson, who has said in an analogous context that “the computer algorithm presents none of the truth-related concerns that arise with a human informant. The computer computes what it computes, neither being true or false.” Ferguson, supra note 16, at 307 n.280. Ferguson’s contention glosses over the important role that human’s play in programming any algorithm and the potential that a programmer’s biases or motives may shade the “truth” of what the algorithm computes.

\textsuperscript{246} See supra note 68 and accompanying text.

\textsuperscript{247} See Joh, supra note 192, at 57 (“Software with a demonstrated history of successfully predicting high crime areas based on verifiable crime data is likely to be a highly persuasive factor in the reasonable suspicion formulation.”).

\textsuperscript{248} See Adams v. Williams, 407 U.S. 143, 146 (1972) (noting that the tip of an informant who had provided an officer “with information in the past” made a stronger case for individualized suspicion than an anonymous tip); Draper v. United
analysis that courts typically undertake when looking at the quality of an informant’s past tips is not robust, with courts often relying on a general assertion of an informant’s reliability by a police affiant. Moreover, the inferences that support giving weight to an informant who has proven reliable – that he has access to information about criminality and reports it truthfully – are quite different from what can be inferred about an algorithm that has proven to be statistically reliable. The former are based on human experience and thus are well within the expertise of police and judges. The latter derive from complex statistical analyses that may not be interpretable by anyone, much less magistrates or officers untrained in statistics. Thus, even though there may be reasons based on a traditional analysis of human motivations to believe that an ASA is “credible” and “reliable,” the traditional informant analysis is a poor fit for the statistical evidence that better substantiates a finding of the proper weight to give to an ASA’s prediction.

The type of data that goes into an ASA’s prediction also does not analogize well to the “basis of knowledge” analysis traditionally used for informant tips. Courts credit human informants whose tips are based on reliable information about a suspect’s criminality. ASAs claim no such inside information; rather, their “tips” are based on an enormous amount of past data about a large number of people and some quantity of data specifically about the suspect. The quality and quantity of this data is

---

249 Goldberg, supra note 40, at 808.

250 Of course, the accuracy of these inferences could be tested empirically and analyzed statistically. The important point, though, is that judges rely on these inferences not because of empirical support they but because they comport with the judge’s intuitions about how people behave.

251 See supra notes 88-91 and accompanying text.

252 See generally Joelle Anne Moreno, Beyond the Polemic Against Junk Science: Navigating the Oceans that Divide Science and Law with Justice Breyer at the Helm, 81 B.U. L. Rev. 1033 (2001) (discussing the challenges of expecting judges to engage in statistical analysis in the context of expert testimony).

253 See Gates, 462 U.S. at 245 (holding that the corroboration of non-criminal details in an anonymous tip suggested that the information came someone who “also had access to reliable information of the Gates’ alleged illegal activities”).

States, 358 U.S. 307, 313 (1959) (police properly relied on information from informant “who information had always been found accurate and reliable”).
central to the weight that should be given to the ASA’s prediction. But the “basis of knowledge” analysis in the informant context provides no insight how an ASA’s prediction should be incorporated into the individualized suspicion analysis.

Finally, corroboration does not provide the same logical basis for believing in an ASA’s accuracy that it does for an informant’s tip. Corroboration of innocent facts in a human informant’s tip, and specifically of the informant’s predictions about the suspect’s future behavior, is relevant because it suggests that the informant has some inside knowledge of the individual’s conduct and thus is more likely to be right about the suspect’s illegal activities. To the extent an officer is aware of the data that resulted in the ASA’s tip, corroboring the accuracy of those data says very little about the accuracy of the ASA’s prediction. Moreover, an ASA will not make any predictions about future behavior outside of the general prediction that the suspect is engaged in criminal conduct. Thus, to the extent there is anything to corroborate, it will not be particularly useful to ensuring the ASA’s accuracy.

To conclude, analogizing an ASA’s prediction to an informant’s tip does not provide a useful analytical structure for courts. Human informants and computer algorithms are fundamentally different in ways that impact how we should assess the reliability of each source of information. As such, courts and police should look elsewhere.

C. Algorithms as Drug-Sniffing Dogs

Like other machine learning algorithms, ASAs are likely to be “black boxes” that take in data and spit out predictions, but whose inner workings are unknown and perhaps incomprehensible to humans. Moreover, the tendency in criminal justice arenas toward secrecy for police investigation strategies suggests that ASAs are unlikely to be transparent or

254 See supra notes 73-76 and accompanying text; see also Ferguson, supra note 16, at 317–18 (discussing concerns about underlying data quality in the context of predictive policing).
255 Gates, 462 U.S. at 244.
256 Supra notes 88-91 and accompanying text.
interpretable. This lack of transparency differentiates suspicion algorithms from traditional algorithms that determine “historical facts,” like DNA matching and blood-alcohol-level testing. The algorithms that underlie these determinations are relatively straightforward and explicable, and therefore they can (at least theoretically) be fully explored through expert testimony and cross-examination. And even if the data used to train an ASA and the rules that the ASA creates were available to a defendant in a suppression hearing, the enormity of the data, the complexity of the rules, and resource constraints would present formidable obstacles to full consideration of how the ASA generated the prediction at issue.

Drug-sniffing dogs are the prototypical black boxes in the individualized suspicion analysis. It is easy to understand that a dog has a heightened sense of smell and that drug-sniffing dogs are trained to recognize certain chemical compounds that are part of or affiliated with illegal drugs. But explaining how the input of the residue of an illegal drug is translated in a dog’s brain into the output of an “alert” is beyond the scope of available expert testimony, in large part because “[t]he science of alerting is not yet fully developed.” Thus, the drug dog’s brain is like an ASA: we know the inputs, and we receive the outputs, but we cannot fully understand how the mechanism works.

257 See Zarsky, supra note 34, at 1526–27.
259 See Kerr, supra note 36, at 875–76.
260 See Myers, supra note 40, at 3–4 (“Researchers at Auburn University studying dogs’ capacity to identify certain smells have found that some dogs can detect odors when the particles in the air are at a concentration of 500 ppt—that’s parts per trillion.”) (emphasis in original); Robyn Burrows, Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files, 19 GEO. MASON L. REV. 255, 280 (2011) (“[A] layman can understand that dogs have a heightened sense of smell and that the dog is trained to detect specific substances.”).
261 Myers, supra note 40, at 4.
The following discussion tests the validity of analogizing ASAs to drug dogs and is divided into two parts. The first outlines the approach taken by courts to drug dogs and some of the criticisms that have been leveled against that approach. The second discusses how the lessons from drug dogs should be applied to ASAs, in light of the similarities and differences between the two.

1. The law of drug dogs

The Supreme Court first touched on the role of drug dogs in the individualized suspicion analysis in United States v. Place. There, the Court dubbed a canine sniff *sui generis* because, at least in an ideal world, it discloses only the presence of contraband, and concluded therefore that it is not a Fourth Amendment search. The Court did not discuss the weight to be given to a drug dog alert in establishing probable cause or reasonable suspicion, though it referred repeatedly to “trained” and “well-trained” canines. In Illinois v. Caballes, a drug dog alerted on the trunk of a vehicle and “[b]ased on that alert,” police searched the trunk. The only question before the Court was whether the Fourth Amendment requires any individualized suspicion before a canine sniff for drugs in permitted. Thus, the Court said nothing about what weight to give a dog’s alert in the individualized suspicion analysis, other than to note that the trial court had found the drug dog’s alert to be sufficiently reliable to create probable cause. Once again, though, the Court referred to “well-trained” drug dogs in formulating its holding, without explaining what might characterize sufficient training for a narcotics dog.

---

263 *Id.* at 707.
264 See, e.g., *Id.* at 705-06 (“Moreover, police may confine their investigation to an on-the-spot inquiry—for example, immediate exposure of the luggage to a trained narcotics detection dog,...”).
266 *Id.* at 406.
267 *Id.* at 407.
268 *Id.* at 409.
269 *Id.* at 409 (“Accordingly, the use of a well-trained narcotics-detection dog ... during a traffic stop, generally does not implicate legitimate privacy interests.”).
Dissenting in *Caballes*, Justice Souter pointed to substantial data suggesting that “[t]he infallible dog … is the creature of legal fiction.”\textsuperscript{270} Souter’s main argument was that a dog sniff should be treated as a Fourth Amendment search, but he conceded that even a fallible dog alert can create reasonable suspicion or probable cause because “the Fourth Amendment does not demand certainty of success to justify a search for evidence or contraband.”\textsuperscript{271} Nonetheless, he recognized that “sniffing averages” differ from dog to dog.\textsuperscript{272}

In light of *Place* and *Caballes*, federal circuit courts uniformly permitted drug dog alerts to establish individualized suspicion and thus justify searches and seizures.\textsuperscript{273} But before finding that a dog’s alert creates probable cause, lower courts often require some evidence of the dog’s reliability, typically in the form of training records or certifications.\textsuperscript{274} The quantum of evidence of a drug dog’s reliability that courts will require before finding the dog’s alert sufficient to establish probable cause is unclear, however, and critics fear in many cases it is too low.\textsuperscript{275} Moreover, there are no uniform standards for the certification of drug dog reliability.\textsuperscript{276}

The Supreme Court recently tackled the question of how much weight should be given to a drug dog’s alert in the individualized suspicion

\textsuperscript{270} Id. at 411-12 (Souter, J., dissenting).
\textsuperscript{271} Id. at 412-13 (Souter, J., dissenting).
\textsuperscript{272} Id. at 411-12 (collecting cases dealing with potential false positives from drug dog alerts) (Souter, J., dissenting).
\textsuperscript{273} See *Myers*, supra note 40, at 18 n.88 (collecting cases).
\textsuperscript{274} See, e.g., *United States v. Sundby*, 186 F.3d 873, 876 (8th Cir. 1999) (“To establish the dog’s reliability, the affidavit need only state the dog has been trained and certified to detect drugs.”); *United States v. Diaz*, 25 F.3d 392, 394 (6th Cir. 1994) (“For a positive dog reaction to support a determination of probable cause, the training and reliability of the dog must be established.”). \textit{But see} *United States v. Williams*, 69 F.2d 27, 28 (5th Cir. 1995) (“Because a showing of the dog’s reliability is unnecessary with regard to obtaining a search warrant, \textit{a fortiori}, a showing of the dog’s reliability is not required if probable cause is developed on site as a result of a dog sniff of a vehicle.”).
\textsuperscript{275} See *Myers*, supra note 40, at 19–24.
analysis in *Florida v. Harris*. The police searched the defendant’s truck on the basis of a drug dog’s alert, and the State put on evidence of both the dog’s and the dog’s handler’s certification and training. The Florida Supreme Court found the State’s evidence insufficient to establish the reliability of the alert and required instead that the State present training and certification records, field performance records, evidence of the handler’s training and experience, and any other objective evidence of the dog’s reliability known to the officer.

The Supreme Court unanimously reversed the lower court’s decision, holding that the “strict evidentiary checklist” created by the Florida Supreme Court runs contrary to the totality-of-the-circumstances approach required by the Fourth Amendment. The Court further opined that courts should place much greater weight on a dog’s training and certification records than on its field performance. The Court noted two problems with reliance on field data. First, field data cannot accurately establish how often a dog fails to detect drugs, because police typically will not search a car if a dog fails to alert on the vehicle. Second, the Court was concerned that a dog may alert on quantities of drugs that are otherwise undetectable, either because they are too well-hidden or too small for police to find. According to the Court, such instances are not errors by the dog but would be labelled as such, and thus field data will overstate false positives. On the other hand, a controlled training environment ensures that false negatives and false positives are accurately recorded because the dog’s trainers know whether drugs are present. Thus, the Court concluded, “[i]f a bona fide organization has certified a dog after testing his reliability in a controlled setting, a court can presume (subject to any conflicting evidence offered) that the dog’s alert provides

---

277 133 S. Ct. 1050 (2013).
278 Id. at 1054.
279 Id. at 1055 (quoting Harris v. State, 71 So.3d 756, 775 (Fla. 2011)).
280 Id. at 1056.
281 Id.
282 *Fla. v. Harris*, 133 S. Ct. at 1056.
283 Id.
284 Id. at 1056-67
probable cause to search.” A training program that evaluates a dog’s proficiency in finding drugs also can establish a dog’s reliability.

*Harris* has been justifiably criticized for a number of reasons. First, and fundamentally, *Harris* perpetuates a problem that has plagued the Court’s consideration of drug dogs from the beginning: the overvaluing of one piece of data—here, the alert of a trained drug dog—in the totality-of-the-circumstances analysis. *Harris* dictates that the reliability of a dog’s alert should be the central (and perhaps sole) focus of a court’s analysis:

If the State has produced proof from controlled settings that a dog performs reliability in detecting drugs, and the defendant has not contested that showing, then the court should find probable cause. If, in contrast, the defendant has challenged the State’s case (by disputing the reliability of the dog overall or of a particular alert), then the court should weigh the competing evidence. … The question... is whether all the facts surrounding a dog’s alert, viewed through the lens of common sense, would make a reasonably prudent person think that a search would reveal contraband or evidence of a crime.

The problem with this approach is that by focusing on drug dog reliability, courts are likely to undervalue other information. Specifically, courts should consider the “prior odds” that the suspect possessed drugs, i.e., the reasonable likelihood that the suspect possessed drugs before the dog alerted. From a statistical standpoint, one can use an equation called Bayes’ Theorem to predict, based on the prior odds and a drug dog’s rates

---

286 *Id.*
287 *Id.*
288 For comprehensive statistical explanations of this concern, see Myers, *supra* note 40, at 12–18; Goldberg, *supra* note 40, at 817–18.
289 130 S. Ct. 1050, 1058 (2013).
290 In this context, these prior odds can be generated by looking at the frequency of the targeted criminal conduct in the general population or specific facts about the defendant. Goldberg, *supra* note 40, at 818.
of false positives and true positives,\textsuperscript{291} the likelihood that the dog’s alert was correct in a given case.\textsuperscript{292} According to Bayes’ Theorem, even an alert from a very reliable dog does not necessarily produce a strong likelihood that drugs will be found. For instance, if a drug dog has a false positive rate of 5\% and a true positive rate of 90\%, the prior odds of finding drugs must have been at 5\% for the dog’s alert to make it more likely than not that drugs would be found.\textsuperscript{293} While the call in \textit{Harris} to look at “all the facts surrounding a dog’s alert” could be read to include the prior odds, the fact that the \textit{Harris} court did not itself look at any facts other than the dog’s reliability make such an examination unlikely.\textsuperscript{294}

Of course, the \textit{Harris} court’s failure to recognize the importance of prior odds does not preclude courts from considering them, but additional obstacles stand in the way of courts wishing to do so. First, it is somewhat counterintuitive that an alert from a dog that is 95\% accurate does not create a 95\% likelihood that drugs will be found.\textsuperscript{295} Thus, courts are unlikely, without persuasion, to look beyond a dog’s accuracy.\textsuperscript{296} Second, judges and police are not trained statisticians, and therefore they may be incapable, at least without additional training, of accurately incorporating

\textsuperscript{291}False positives are instances when the dog alerts when there are no drugs present, and true positives are instances when the dog alerts when drugs are present. In other words, the false positive rate describes how frequently the dog alerts when it should not, and the true positive rate describes how often the dog alerts when it should.

\textsuperscript{292}Indeed, the totality-of-the-circumstances test for individualized suspicion essentially asks courts to engage in a Bayesian analysis of all new evidence. Max Minzner, \textit{Putting Probability Back into Probable Cause}, 87 \textit{Tex. L. Rev.} 913, 920 n.32 (2009).

\textsuperscript{293}Id. at 950 n.181.

\textsuperscript{294}For instance, in \textit{Harris} the defendant was pulled over for an expired license plate, was visibly nervous, unable to sit still, shaking, and breathing rapidly, and had an open can of beer in his cup holder. 133 S. Ct. 1050, 1053 (2013). It is possible that these background facts established prior odds of drug possession sufficiently high for the dog’s alert to establish probable cause, but that conclusion is not obvious, and the Court did not ask the question. \textit{See also} Minzner, \textit{supra} note 292 at 950 n181 (noting the differences in the background facts, and likely prior odds, in \textit{Place and Caballes}).

\textsuperscript{295}\textit{See} Myers, \textit{supra} note 40, at 13.

\textsuperscript{296}This likely explains why, even before \textit{Harris}, lower courts accepted a drug dog’s alert as sufficient to establish probable cause. \textit{See supra} note 273.
prior odds into their individualized suspicion analysis. Third, prior odds often are unavailable. Fourth, unless they apply statistical formulae like Bayes’ Theorem, police, magistrates, or courts who receive numerical probability data, like a dog’s accuracy rate, are likely to give it undue weight because of the “anchoring effect,” or the human tendency to grab hold of any available number as the starting point in the face of uncertainty. For instance, a court may use a drug dog’s 95% hit rate as a starting point in the probable cause analysis and adjust up or down from there, without understanding that because of low prior odds, the actual likelihood of finding contraband was far lower.

In addition to this fundamental flaw, the Harris court also relies on two questionable factual premises: first, that training and certification programs are strong evidence of a dog’s reliability; and second, that field performance is weak evidence of reliability. The first claim itself is faulty for two reasons. First, there are no accepted standards for dog training. Dogs are trained according to standards articulated by the relevant law enforcement agency, or they may be certified by private organizations. The reliability required for a dog to achieve certification varies substantially among the regimens. The most stringent require 100 percent accuracy, while some certify police dogs that are reliable in controlled testing environments only 70 percent of the time. Of course, a certification is only as strong as the underlying testing standards, and the absence of such standards should give courts pause as they assess even a certified dog’s reliability.

---

297 See Minzner, supra note 292, at 952–56 (discussing “capacity objections” to the use of statistical evidence that are based on the inability of decision makers to accurately consider such evidence).
298 Taslitz, supra note 115, at 862–63 (noting that generalized, objective probability data regarding crime rates are rarely available).
300 Harris, 133 S. Ct. at 1056-57.
302 Bird, supra note 276, at 420–21.
303 Phipps, supra note 301, at 78.
304 Id.
The second problem with giving great weight to training certification is that a dog’s reliability in a controlled testing environment fails to account for circumstances in the real world that cause a drug dog to alert falsely. Conscious or unconscious cues from a dog’s handler may cause the dog to alert falsely. Because of poor training or temperament, a drug dog may get distracted by chaotic, real-world circumstances. A dog can be trained to ignore distractions, and a handler can be trained not to cue their dog, but a training certification does not provide any information about how well the dog and handler apply that training in practice.

Meanwhile, the Court’s second premise—that field performance is a poor indicator of reliability—is based on a misunderstanding of the probable cause requirement. Specifically, the Court argues that a dog’s alert on the residual odor of drugs when no contraband is actually present is not a false positive that undermines the dog’s reliability. Yet, “probable cause to search requires an assessment of the odds that evidence is currently located in the place to be searched, not that it was there at some indeterminable time in the past.” Moreover, while the Court is right that field records cannot accurately record when a dog fails to find drugs that are present, such false negatives are not what matter when it comes to individualized suspicion. The Fourth Amendment protects individuals against unreasonable searches and seizures, not from searches and seizures that did not happen. Thus, field records are highly relevant evidence of

305 Myers, supra note 40, at 22–24.
306 Id. at 4.
307 See Bird, supra note 276, at 413–14.
308 Harris, 133 S. Ct. at 1056–57.
309 Kinports, supra note 41, at 68; see also Phipps, supra note 301, at 76–77 (“Although detecting residual odors from weeks prior may seem like a valuable trait in a dog, it actually demonstrates that the dog is less reliable at discerning whether drugs are actually present.”); Myers, supra note 40, at 22 (“Perversely, the better the dog is at detecting trace amounts of the desired substance, the higher the likelihood that the dog will alert on trace amounts that are inadvertently present in materials owned by the innocent.”).
310 See Myers, supra note 40, at 15.
what matters in terms of a dog’s reliability: how often a drug dog’s alert accurately predicts the presence of contraband.\textsuperscript{311}

Finally, critics point out that even though \textit{Harris} requires courts to consider evidence that might undermine drug dog’s reliability,\textsuperscript{312} the defense is unlikely to have access to such information.\textsuperscript{313} Police agencies often do not keep detailed records of drug dog performance in the field.\textsuperscript{314} Even when they do, such records, and other relevant evidence like training details, are generally in the hands of the government, and defendants are likely to have a difficult time obtaining them in discovery.\textsuperscript{315} Thus, \textit{Harris} may, for all practical purposes, create a bright-line rule that a drug dog’s alert creates probable cause.\textsuperscript{316}

2. ASAs as drug dogs

As just explained, courts trying to decide whether a drug dog’s alert created individualized suspicion are instructed to look at a drug dog’s training reliability, any certifications, its field performance, and any facts about the specific alert.\textsuperscript{317} Analogizing an ASA to a drug dog, a court determining whether an ASA’s prediction created individualized suspicion would look at the strength of ASA’s prediction, the confidence level of that prediction as established in initial programming of the ASA, the ASA’s field performance, and any specific facts about the prediction to determine if sufficient individualized suspicion existed.

This analogy brings good news and bad news. The good news is that considering an ASA like a drug dog requires courts and police to ignore what they are ill-equipped to evaluate. Courts are not expected to directly examine for soundness the biological processes in a drug dog’s brain by which drug residues inhaled by the dog result in an alert. Similarly, courts

\textsuperscript{311} See Phipps, supra note 301, at 73–75 (collecting studies documenting drug dog accuracy based on field studies).
\textsuperscript{312} Harris, 133 S. Ct. at 1057.
\textsuperscript{313} Kinports, supra note 41, at 65–66.
\textsuperscript{314} \textit{Id.} at 65.
\textsuperscript{315} \textit{Id.} at 65–66.
\textsuperscript{316} \textit{Id.} at 65.
\textsuperscript{317} Harris, 133 S. Ct. 1050, 1057-58 (2013).
would not be expected to directly examine what an ASA does with the information it receives in order to create its predictions of criminality. This is good news because, as explained earlier, the most effective ASAs are likely to operate in a way that is not comprehensible even to the people who programmed the algorithm. Instead, courts considering a drug dog’s alert assign weight to the alert based on the quality of the inputs and the outputs. Courts treating ASAs like drug dogs would do the same.

The bad news is that the flaws in the drug dog analysis may work even greater mischief if that analysis is applied to ASAs. First, the problem of prior odds remains, but it is more complicated with respect to ASAs. The prior odds are important to the individualized suspicion analysis for a drug dog alert, because the facts that go into calculating those odds are not part of the reliability information about the dog’s alert. In other words, the facts underlying the prior odds are independent of the reliability of the dog’s alert. For instance, the fact that the police stopped Harris for driving with an expired license plate is independent from the dog’s reliability, because the reliability of a dog’s alert generally will not be calculated based on the reasons behind a given stop. Thus, the reason for the stop should be included in the prior odds calculation, i.e., a court should consider how much, if at all, the fact that a vehicle was stopped for an expired license plate increases or decreases the likelihood that drugs would be found in the vehicle. On the other hand, if we know the reliability of a dog’s alert when that dog alerts on a truck rather than a car, then the fact that Harris was driving a truck is not independent of the dog’s reliability and should not be incorporated into the prior odds calculation.

Identifying the evidence that is independent of a dog’s reliability is easy, because that reliability is likely going to be described in basic terms like, “Bobo correctly alerted 71% of the time.” Thus, in most cases any facts

318 See supra note 91 and accompanying text.
319 See Minzner, supra note 292, at 921 (recognizing that for new evidence to impact the accuracy of a probable cause determination, the evidence must not have already been considered in the pre-existing probable cause analysis).
320 See Harris, 130 S. Ct. at 1053.
321 See id.
322 United States v. Kennedy, 131 F.3d 1371, 1378 (10th Cir. 1997).
specific to an individual alert should contribute to the calculation of prior odds. On the other hand, the strength of an ASA’s prediction may be based on a substantial and unknown network of facts. Imagine, for instance, that an officer receives a prediction from an ASA that a suspect on a street corner has a 62% of being engaged in drug dealing. When the officer approaches the suspect, she will necessarily learn facts about the suspect. Perhaps she will know from walking the beat that the suspect is a local pastor, or she may observe the color of the clothing he is wearing. She must then decide whether the totality of the circumstances creates individualized suspicion that permits her to seize the suspect. But unless the facts that she observed were not included in the ASA’s calculation of the strength of its prediction, the officer should not consider them when determining whether to rely on the prediction in finding individualized suspicion to seize the suspect. Otherwise, those facts will be double-counted.

For two reasons, however, it will be difficult, or even impossible, for the officer to know whether the facts she learned were considered by the ASA, however. First, ASAs can process massive amounts of data, and police may not even know what kind of data is input into an ASA. For instance, is clothing color a feature considered by the ASA? If not, the officer should incorporate her observations of clothing color in her analysis; if so, she should not because it has already been considered. This problem is at least theoretically solvable by ensuring that police agencies and individual officers are informed about the types of information used by an ASA. Second, there may be no way for an officer to know what information the ASA actually obtained about this suspect in making its prediction. In this case, even if an individual’s occupation is a feature in the ASA’s model, did the ASA make a positive identification of the suspect and “know” that he was a pastor before making its prediction? Again, if not, the officer should incorporate that information in her analysis; if so, she should ignore it because it has already been considered. Whether the officer can access this information will depend on whether

323 Note that the reliability of the drug dog is analogous to the numerical certainty expressed by the ASA in its prediction of criminality.
324 See Goldberg, supra note 40, at 833 (discussing the problem of double-counting in the context of a facial recognition device).
and to what extent the ASA is interpretable. Without interpretability, it will be impossible for the officer to make an accurate assessment of individualized suspicion. Moreover, even if this information is available, it must be constantly communicated to officers acting on the prediction.

Second, relying only on training performance and certification to assess the reliability of ASAs is problematic for a couple of reasons. The first is that the programming of ASAs is far more complex than the training of drug dogs. Teams of programmers will inevitably make hundreds or thousands of decisions throughout the programming process, and each of these decisions may create errors in the ASA. This complexity ratchets up the importance of robust, meaningful standards for the creation and training of ASAs that minimize ASA error and maximize effectiveness. Only with such standards can certification of an ASA provide substantial guarantees of accuracy in the individualized suspicion analysis. Unfortunately, the unconcern that the Court showed in Harris about certification standards provides little reason to believe that courts would require more from ASAs.

Even with robust certification procedures, field performance data are crucial in the evaluation of an ASA’s reliability. A dog sniff is a straightforward process: a dog sniffs air to determine whether it contains trace amounts of narcotics. Though the circumstances in which a drug dog and handler seek to achieve this goal can vary substantially, the input and task remain essentially the same. The input and task of an ASA, on the other hand, vary substantially depending on circumstances and over

325 See supra notes 79-87 and accompanying text (discussing sources of error in machine learning algorithms).
326 See Florida v. Harris, 133 S.Ct. 1050, 1054 (2013) (finding dog’s training sufficient based on its quantity and reports that the dog performed “really good” and “satisfactorily” in training).
327 In fact, criminals try to make the drug dog’s job more difficult by, for example, masking the odor of illegal drugs with some other substance, such as talcum powder or perfume. See David S. Rudstein, “Touchy” “Feely” – Is There a Constitutional Difference? The Constitutionality of “Prepping” a Passenger’s Luggage for a Human or Canine Sniff after Bond v. United States, 70 U. Cin. L. Rev. 191, 200 (2001) (describing methods used by criminals to mask the scent of drugs). If criminal avoidance methods do change substantially over time, that presents yet another argument for the use of field performance records in the drug dog context.
time. The same crime may be committed in different ways in different places. Thus, the data used to train an ASA may not lead to reliable results in all places. More importantly, how crimes are committed change over time, particularly in response to law enforcement activities. Consequently, even with robust, accurate, and representative training data, changes in crime patterns over time will inevitably lead to less reliable predictions. This diminishing reliability can only be captured through field performance data. Therefore, even crediting the Harris Court’s critique of field performance data in the dog sniff context, courts and police must consider field performance data when assessing the reliability of an ASA’s prediction.

Finally, just as the state holds the data needed to undermine a drug dog’s reliability, so too will the government likely possess the information that a defendant would need to challenge an ASA’s prediction in court. In particular, a defendant would want information about: (1) an ASA’s reliability in general, including about any certification it received, its training performance, and its field performance, and (2) the ASA’s application to the defendant’s case, including the facts that the ASA incorporated into its analysis and how those facts were used. Access to all of these facts would be necessary to ensuring the most robust individualized suspicion argument.

Yet prosecutors are likely to resist the disclosure of information about how an ASA works on the ground that such information may be used by criminals to “game the system” by avoiding in engaging in conduct that

328 This is an example of an error that would arise from training data not being sufficiently representative of real-world situations. See supra notes 77-78 and accompanying text. But even if training data is representative, an ASA may be particularly unreliable in geographical locations with peculiar crime patterns. 329 See William J. Stuntz, Race, Class, and Drugs, 98 COLUM. L. REV. 1795, 1804 (1998) (noting, with respect to illegal drug sales, that “as soon as law enforcement agencies adapt to a particular distribution pattern, the sellers have an incentive to change the pattern. The result is a cat-and-mouse game, with different forms of a given drug sold by different actors in different ways at different times and place.”). 330 Moreover, assessing the reliability of an ASA over time is the only way to ensure that the ASA continues to learn from new data and improve.
the ASA uses as a proxy for criminality.\textsuperscript{331} This argument has substantial currency under the law,\textsuperscript{332} but it does not apply with the same force to all kinds of information that a defendant may want. Generalized information about certification and reliability, for instance, reveals nothing about how an ASA works and would provide no guidance for future criminals seeking to avoid detection. Therefore, this information should be provided to defendants. Similarly, knowing the types of information that an ASA incorporates into its analysis may of limited utility to future criminals, but without knowing more about which facts matter and how they matter, criminals trying to alter their behavior to escape suspicion will be stumbling in the dark. Most useful to future criminals would be information about the specific facts relevant to a prediction and data about how the ASA weighs those facts. With such information, criminals could change their behavior in targeted weights to avoid detection. Thus, such information is the most deserving of protection on this ground.\textsuperscript{333}

3. Conclusion

While drug dogs are the best analogy in current Fourth Amendment jurisprudence to ASAs, a number of lessons emerge from the application of this analogy. First, courts must recognize that an ASA’s prediction,

\textsuperscript{331} See Zarsky, \textit{supra} note 34, at 1554. Prosecutors also may argue that information about ASAs is a trade secret that must be protected from disclosure. See Danielle Keats Citron, \textit{Technological Due Process}, 85 WASH. U. L. REV. 1249, 1291-93 (discussing trade secret arguments against disclosure by government attorneys in other contexts); see also David S. Levine, \textit{Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure}, 59 FLA. L. REV 135 (2007) (discussing trade secrecy relating to governmental function, such as voting machines). ("While many people may not give [government secrecy] much thought, it is difficult to ignore such concerns because we interact with this infrastructure—roads, the Internet, governmental actions like law enforcement—on a daily basis."). The arguments for and against this position are beyond the scope of this Article.

\textsuperscript{332} \textit{Id.}

\textsuperscript{333} \textit{Id.} at 1555 ("Yet perhaps the most salient context for this pro-opacitv argument is elsewhere in the “usage” stage—at the point at which the government uses a mix of criteria, factors, behaviors, and attributes as proxies to identify wrongdoings. Here, the opacity argument is perhaps most intuitive—if government discloses the lists of proxies used, adversaries will simply avoid these proxies. They will, however, still engage in unlawful conduct. Therefore, providing information regarding these steps of the process should be prohibited.").
like any prediction of criminality, is only a part of the totality-of-the-circumstances analysis, and litigants must be prepared to educate courts about the importance of facts other than an ASA’s numerical prediction in determining the existence of individualized suspicion. Second, interpretability of ASAs remains a central issue. While a “black box” ASA is more likely to provide accurate predictions, information about how an ASA works is necessary for the most accurate and complete Fourth Amendment analysis. Experts in relevant fields, like machine learning, law, and law enforcement, should come together to consider how to balance these concerns most effectively. Third, as ASAs become more widespread, these same subject-matter experts must work together to propagate standards for the development of accurate and effective ASAs. In addition, courts must require ASAs to be certified in accordance with these standards before an ASA’s prediction can be used to establish individualized suspicion, or at least weight the absence of a certification heavily in the individualized suspicion analysis. Fourth, police agencies must maintain data about the performance of ASAs in the field; similarly, ASA standards should mandate that ASAs be programmed to make the collection of such data straightforward. Finally, on a case-by-case level, defendants must be prepared to argue for full disclosure of training and field performance data for ASAs, as well discovery into the kinds of data that the ASA uses. Courts, in turn, must be willing to ordering disclosure of this information despite prosecution arguments to the contrary.

334 Given the Court’s disfavor of bright-line rules, requiring certification may be implausible without legislation. See Florida v. Harris, 133 S.Ct. 1050, 1055 (2013) (“We have rejected rigid rules, bright-line tests, and mechanistic inquiries in favor of a more flexible, all-things-considered approach.”).

335 This same recommendation has been made with respect to drug dogs, see Myers, supra note 40, at 33.

V. ASA Errors

The previous Parts established that ASAs do not replace the role of people in making the determination of whether probable cause or reasonable suspicion exists, but that they can be considered, with some caveats, as similar to drug dogs in the totality-of-the-circumstances analysis. A question remains, however: what if an ASA is wrong?

Before answering this question, though, it is important first to define when an ASA is “wrong.” Specifically, an ASA is not “wrong” every time an officer searches or seizes a suspect in reliance on an ASA’s prediction and finds no evidence of criminal conduct. Like any predictive machine learning algorithm, an ASA can make only probabilistic predictions. Indeed, probable cause and reasonable suspicion are themselves probabilistic predictions, and in a given instance a search or seizure based on the existence of probable cause that does not ultimately lead to the discovery of criminal conduct is not a Fourth Amendment violation. Rather, an ASA is wrong when it provides a prediction of criminality that it should not have provided. Such error can arise in two general ways: first, the ASA could be working with inaccurate data; or second, the ASA’s error could arise from human error of some kind during the programming process. Of course, for Fourth Amendment purposes, we only care about false positives, where an innocent person is predicted to a

---

337 Remember that machine learning algorithms inevitably learn approximations of complex underlying phenomena (like whatever causes individuals to commit crimes). See supra notes 70-72 and accompanying text. Thus, errors, in the sense of probabilities that do not pan out in particular instances, are inevitable.

338 See United States v. Arvizu, 534 U.S. 266, 277 (2002) (“A determination that reasonable suspicion exists, however, need not rule out the possibility of innocent conduct.”).

339 For example, if an ASA predicts a 60% chance that an individual is engaged in a certain criminal conduct, but the ASA should have predicted a 34% of criminality, then the ASA’s prediction was wrong.

340 See supra notes 73-78 and accompanying text.

341 See supra notes 79-87 and accompanying text.
criminal, because in those instances alone will police search or seize someone.\footnote{False negatives matter, too, because we want police to catch criminals and prevent crime, but they do not false within the scope of the Fourth Amendment’s protections.}

The Supreme Court handles issues of error under the “good faith” or “reasonable reliance” doctrine. The doctrine was born in the case of \textit{United States v. Leon},\footnote{\textit{Id.} at 922.} in which the Court found that evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant would not be subject to the exclusionary rule.\footnote{\textit{Id.} at 922.} In \textit{Arizona v. Evans},\footnote{\textit{Id.} at 15-16.} the Court extended the doctrine into the digital realm, holding the exclusionary rule inapplicable to evidence found during an unconstitutional search conducted in reasonable reliable on an incorrect database entry that a judicial court clerk had failed to correct.\footnote{\textit{Id.} at 135 (2009).}

Then, in \textit{Herring v. United States},\footnote{\textit{Id.} at 138.} the Court applied the doctrine to refuse to suppress evidence obtained during an unconstitutional search undertaken in reliance on an expired warrant.\footnote{\textit{Id.} at 138.} The warrant had been recalled five months earlier, and a law enforcement official had failed to update a warrant database to reflect the recall.\footnote{\textit{Id.} at 138.} While the database error itself was negligent, the searching officer’s reliance on the database was objectively reasonable.\footnote{\textit{Id.} at 138.} The Court explained that when an error is “attenuated” from the search or seizure, such as an error in entering data or maintaining a database, the exclusionary rule will apply only if the error is “deliberate, reckless, or grossly negligent”, or it involves “recurring or systemic negligence.”\footnote{\textit{Id.} at 144.} Thus, because the database error was attenuated from the arrest, the negligence of the law enforcement official in...
maintaining the database did not require suppression of the evidence.\textsuperscript{352} Moreover, the defendant’s failure to show that errors in the warrant database were “routine or widespread” meant that the evidence would not be suppressed on that ground.\textsuperscript{353} Finally, the arresting officer’s reasonable reasonableness in relying on the information he received about the warrant also did not require suppression per \textit{Leon}.\textsuperscript{354}

While the precise impact of \textit{Herring} on Fourth Amendment doctrine is unclear,\textsuperscript{355} its application to ASA errors is straightforward. Certainly, if a police employee’s error in \textit{Herring} was “attenuated” from the arrest, the provision of bad data to the ASA or mistakes in programming it also would be attenuated from any search or seizure.\textsuperscript{356} Thus, any ASA errors would require suppression only if they were the result of deliberate, reckless, or grossly negligent misconduct, or routine or systemic negligence.

This easy application of the doctrine glosses over looming concerns about the practical impact of \textit{Herring} on the regulation of ASAs, however. In dissent, Justice Ginsburg presciently recognizes the impact of the Court’s holding on more far-reaching and complex computer systems than the manual-entry warrant system before the Court. She notes first that “[e]lectronic databases form the nervous system of contemporary criminal

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{352} \textit{Id.} at 146.
\item \textsuperscript{353} \textit{Id.} at 147. Though the Court presents the absence of this evidence in the passive voice, \textit{id.} ("But there is no evidence that errors in Dale County’s system are routine or widespread."), the failure clearly lies with the defendant, who would be expected to provide such evidence.
\item \textsuperscript{354} \textit{Id.} at 146.
\item \textsuperscript{355} \textit{See} Jennifer E. Laurin, \textit{Trawling for Herring: Lessons in Doctrinal Borrowing and Convergence}, \textit{COLUM. L. REV.} 670, 672 (2011) ("The academic response to \textit{Herring} has by and large been negative; however, to date, it has consisted as much of general puzzlement as critique.").
\item \textsuperscript{356} Unfortunately, the \textit{Herring} court provides no definition for “attenuation” in its opinion. \textit{See Id.} at 687 ("Assessing the limiting work done by the Court’s references to ‘attenuation’ is complicated by the opinion’s silence as to the meaning of the term."). As used in \textit{Herring}, however, attenuation does not seem to require the passage of time, intervening events that make a finding of “but-for” causation too remote, or “a disconnect between the constitutional interests protected and the harm suffered by the defendant.” \textit{Id.} at 687–88.
\end{enumerate}
\end{footnotesize}
justice operations.” Yet, such systems are inadequately monitored and contain numerous errors. Moreover, if a defendant must show deliberate, reckless, or grossly negligent conduct, or routine or systemic errors, to get relief in cases of computer errors, then the defendant must be provided with discovery or even an opportunity to audit police databases in order to prove them. Finally, without some threat of evidence being suppressed, police may not have sufficient incentives to maintain accurate databases and computer systems.

In a similar vein, Erin Murphy has articulated a number of “shared features that inhere across databases generally,” some of which are applicable to ASAs. First, she recognizes that databases are best regulated at a structural level, rather than on a case-by-case basis. This is because databases are constructed by numerous people, spread out across time and geography, with different roles and motivations. A single defendant and her counsel do not have the resources, or the motivation, to stare down this massive, interlocking structure, see the problems, and push for large-scale solutions. Second, Murphy observes that databases “tend to operate anonymously” and their “content is typically shrouded in secrecy.” Litigation, as a presumptively public event, runs contrary to this obscurity, and thus “[i]t is too much to require courts, or to expect the Constitution, to demand full transparency in the methods of database administrators.” Finally, Murphy notes that “it is far easier to do harm, and far greater harm can be done, through mere

357 Herring, 555 U.S. at 155 (Ginsburg, J., dissenting).
358 Id. (Ginsburg, J., dissenting); see also Christopher Slobogin, Government Data Mining and the Fourth Amendment, U. Chi. L. Rev. 317, 324 (2008) (“Most fundamentally, the information in the records accessed through data mining can be inaccurate.”).
359 Herring, 555 U.S. at 157 (Ginsburg, J., dissenting).
360 Id. at 156 (Ginsburg, J. dissenting).
361 Murphy, supra note 26, at 826.
362 Id.
363 Id. at 827–28.
364 See Id. at 829 (“Discovery, compulsory process, or cross-examination in a single case yields little opportunity to identify and uncover, much less broadly correct, errors apt to occur (and be visible) only from scrutiny on a systemic level.”).
365 Id. at 831.
366 Id. at 832.
benign neglect of database systems than through intentional manipulation.\textsuperscript{367}

If unregulated, the police use of ASAs is likely to display the concerns of Justice Ginsburg and the observations of Professor Murphy in full bloom. By encroaching on the second step of the individualized suspicion analysis, ASAs can truly become the “nervous system” of the criminal justice system. Unless forced into interpretability, an ASA’s operations are not just obscure; they are completely opaque, such that inquiry into them would not only be difficult or unfeasible for defendants, but impossible. Moreover, ASAs can potentially analyze so much data that discovery of the underlying databases would overwhelm even the most industrious and well-funded defense counsel. As a result, an ASA’s individual prediction errors would be difficult to uncover in most cases. And even if an ASA’s errors could be found, it would be effectively impossible for a defendant to make the showing of either willful misdeeds or routine errors that would be necessary for suppression of evidence and any hope of encouraging reform. Thus, bad data and benign neglect could flourish in the ecosystem of an ASA if the only oversight comes from case-by-case Fourth Amendment adjudication.\textsuperscript{368}

The certainty of ASA errors, therefore, militates in favor of systemic oversight. Again, as in the previous part, the creation of standards governing the programming of ASAs by experts in relevant subject-matter fields, such as machine learning, law, and law enforcement, is of paramount importance. These standards should cover the training and programming of the ASAs, as well as some continued oversight to ensure that ASAs learn from new data so that errors are minimized and effectiveness is maximized. Standards alone are not enough, however. Courts also must be willing to require ASAs to meet these standards and to exclude evidence obtained based on ASAs that do not. In particular, courts must not require defendants to make the almost-impossible showing that an ASA’s specific failure to meet the standards led to some articulable

\textsuperscript{367} Id. at 835.
\textsuperscript{368} See also Citron & Pasquale, supra note 6, at 1481–83 (discussing political reasons why courts may be ineffectual in monitoring “fusion centers” that accumulate and use massive amounts of data in counterterrorism).
harm to the defendant.\textsuperscript{369} Fortunately, \textit{Herring} continued to limit the good faith exception to the exclusionary rule to situations where police act in objectively reasonable reliance on the evidence in question.\textsuperscript{370} Courts should give teeth to this limitation by recognizing that when ASA standards exist, reliance by police on an ASA that does not meet those standards is unreasonable.

\textbf{VI. CONCLUSION}

The overarching lesson of the preceding discussion is that ASAs are not an easy fit for existing Fourth Amendment doctrine. While it is possible that courts will undertake the “major reorientation in constitutional thinking” that ASAs and similar networked technologies demand,\textsuperscript{371} such a substantial shift seems unlikely, at least before ASAs enter the mainstream. Instead, police, magistrates, and litigants must find ways to analyze them logically within existing doctrine. This Article provides a beginning framework for that analysis. First, though ASAs intrude on the second step of the individualized suspicion analysis, they cannot replace a human being when it comes to consideration of the totality of the circumstances in each case. Instead, their predictions are merely another fact, albeit perhaps a quite weighty one, in that analysis. Second, an ASA’s predictions are best analogized to a drug dog’s alert in the totality of the circumstances analysis. Unfortunately, flaws in current Supreme Court doctrine on drug dogs and the unique characteristics of ASAs suggest that more work needs to be done by legal scholars and experts in machine learning, law, and policing. In particular, uniform and robust standards are needed for the programming, training, and continued use of ASAs, including monitoring of the data used by ASAs, to maximize ASA accuracy and minimize errors resulting from bad data and programming errors. In addition, courts must be prepared to give defendants latitude in

\textsuperscript{369} \textit{See} Murphy, \textit{supra} note 26, at 822–23 (noting that the normal requirement of proof of a specific articulable harm to the defendant from a database may be impossible to meet because of the diffuse and decentralized nature of databases and the incentive of those in charge of the database to protect themselves from blame).

\textsuperscript{370} \textit{Herring} v. United States, 555 U.S. 135, 142 (2009) (“the exclusionary rule does not apply if the police acted in objectively reasonable reliance on the subsequently invalidated search warrant”).

\textsuperscript{371} Murphy, \textit{supra} note 26, at 829.
their questioning of ASA reliability and to exclude evidence obtained as a result of officer reliance on uncertified ASAs or ASAs that are not proven to be reliable.