PREDICTIVE POLICING: THE ARGUMENT FOR PUBLIC TRANSPARENCY

*ERIK BAKKE**

* J.D. 2018, New York University School of Law. Special thanks to Professors Barry Friedman and Maria Ponomarenko, as well as the Policing Project. Additional thanks to Natalie C. Gow and the entire editorial staff at the *Annual Survey of American Law* for all of their input and efforts preparing this Note for publication.

INTRODUCTION

At 4 p.m. on a Tuesday in Santa Cruz, the officer's squad car radio reports a robbery. The officer puts his car in gear and radios back his pursuit of the robber.[1] After making a few turns, he catches up to the suspect running from the scene just moments after receiving the initial report. The officer's success is not due to luck, but to the Santa Cruz Police Department's (SCPD) predictive policing system. Santa Cruz receives a significant amount of tourism, and with that tourism comes a substantial amount of street crime. Fast response times are crucial for tracking down suspects. Looking to improve response times, the SCPD contracted with PredPol, a private company, to purchase predictive policing technology.

PredPol's technology, like competing predictive policing tools, uses computing and analytics to make predictions about where and when crimes are most likely to occur. The PredPol system estimates the likelihood of four crimes (auto theft, vehicle burglary, burglary, and gang-related activity) each day for fifteen zones. Each zone covers a precise area of only 500 by 500 feet. The SCPD uses those predictions to determine where to station its officers.

Police departments using predictive technologies hope they will improve their departments' effectiveness. PredPol allows the SCPD to pursue that goal without any additional hires, which its budget does not allow. The system is not the only new measure Santa Cruz is implementing to try to improve policing. The SCPD has also instructed officers to engage more with the community and forge more relationships with locals as they patrol, but PredPol remains a substantial part of the city's plans for improving police tactics.

PredPol is just one of many predictive policing algorithms available for purchase, and Santa Cruz is just one of many police departments to have adopted the technology. Predictive policing devices and technologies are growing in popularity among law enforcement departments, with thirty-eight percent of police depart-

1. The introductory story and application in Santa Cruz come from an article by Eyragon Eidam, *The Role of Data Analytics in Predictive Policing*, GOV'T TECH. (Sep. 2016), http://www.govtech.com/data/role-of-data-analytics-in-predictive-policing.html.

ments currently using predictive policing and seventy percent expecting to implement it in the next two to five years.[2] But as their popularity is increasing, so too are concerns about the potential downsides of the technology. Law enforcement and the public are not entirely aware of every hazard that will accompany predictive policing technologies. Due to the highly technical nature of predictive policing, public transparency should be a priority. While real-time predictions of crime locations must be withheld for the technology to provide any real benefit, police should at the very least reveal algorithm inputs, algorithms, and obsolete predictions whenever possible if employing predictive policing.

In Section I, I describe what predictive policing is, its benefits, and its drawbacks. I also explain how law enforcement typically purchases the technology from private developers and why private development raises concerns about information asymmetry.

In Section II, I describe the most common arguments for and against predictive policing. In Section III, I add my own arguments. First, arguing the importance of transparency specific to predictive policing, I contend transparency provides a critical democratic check for predictive policing. Second, I argue that transparency can increase law enforcement effectiveness in jurisdictions with predictive policing through increased legitimacy and deterrence. Finally, I propose that transparency allows the public to demand change in cases where flawed algorithms arbitrarily distribute the costs of enforcing the law.

In Section IV, I describe the current apparatus through which the public can request transparency from the government. Open records laws, at the federal and state level, require the government to provide answers upon request from citizens, but they also contain a number of exceptions. Here, the business information and law enforcement exceptions both provide potential avenues for denying public information requests.

---

2. Office of Cmty. Oriented Policing Servs., U.S. Dep't of Justice, Future Trends in Policing (2014).As a whole, the predictive analytics industry is expected to grow from USD $ 3.49 billion to $10.95 billion by 2022. Zion Market Research, *Trends in Predictive Analytics Market Size & Share will Reach $10.95 Billion by 2022,* GlobeNewswire (Mar. 2, 2018), https://globenewswire.com/news-release/2018/03/02/1414176/0/en/Trends-in-Predictive-Analytics-Market-Size-Share-will-Reach-10-95-Billion-by-2022.html [https://perma.cc/99RP-LMJC]. Over 60 U.S. police departments currently use some form of predictive policing. Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement(2018).

I.
PREDICTIVE POLICING

Predictive policing is the application of analytical techniques to identify where crime is likely to occur and who is likely to commit crime.[3] It refers to both traditional methods of distributing law enforcement resources where departments believe they will most be needed and modern predictive algorithms and codes, the latter of which are the focus of this article.[4] This section defines the modern high-tech approach to policing, weighs its benefits against its risks, and describes how law enforcement usually obtains predictive policing technology.

A. Summary of Predictive Policing Technology

Predictive analytics rely on "sophisticated computer programs, extensive data sets, and professional data analysts."[5] Advanced technology helps to "uncover non-obvious relationships" and make predictions that were previously impossible.[6] One of predictive policing's most distinctive characteristics is its ability to predict future behavior from past data, moving beyond the dataset of past crimes.[7] Consider a town with one hundred convenience stores. Old predictive methods could use previous robberies at three convenience stores to predict future robberies at those stores or stores near them. A new predictive policing algorithm might combine past crimes with other data to inform officers of a greater chance of a robbery occurring at a fourth convenience store across town. The technology provides a more granular prediction, and algorithms al-

3. *See id.* at 1 (defining predictive policing). In 2009, the National Institute of Justice defined it as "taking data from disparate sources, analyzing them, and then using the results to anticipate, prevent and respond more effectively to future crime." Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, 266 NIJ J. 16, 16 (2014).

4. *See generally,* WALTER L. PERRY ET AL., PREDICTIVE POLICING 9 (RAND Corporation 2013).

5. Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1510 (2013).

6. PERRY, ET AL., *supra* note 4, at 2; *See also,* Andrew G. Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 281–84 (2012) (discussing how near repeat theory and risk terrain modeling in predictive policing makes predictions otherwise impossible without advanced technology).

7. *See* Shaun B. Spencer, *When Targeting Becomes Secondary: A Framework for Regulating Predictive Surveillance in Antiterrorism Investigations*, 92 DENVER U. L. REV. 493, 499 (2015).

ready exist that can predict crimes based on likely location, offender, victim, and time.[8]

The predictive power of these algorithms hinges on both the analyst's role in designing the model and the data input. Analysts often take an "active role in defining the parameters of the actual data-mining analysis and the creation of clusters, links, and decision trees which are later applied."[9] This allows analysts to influence which variables algorithms take into account[10] and engrain their positive and normative decisions into future predictions. However, algorithm design is only half the story. Without representative data, even a perfectly-designed algorithm is unable to make predictions that accurately reflect the situation on the ground.[11] Expecting the algorithm to perform properly under these conditions would be like expecting Google Maps to find your destination after you typed in the wrong address.

When well-designed and backed by good data, predictive policing algorithms have been a boon to a number of law enforcement goals: overcoming budget restrictions, increasing surveillance, and preventing crimes before they occur. First and foremost, algorithms allow departments to get more out of a smaller force, cutting crime without significantly expanding budgets.[12] For example, the "Blue Crush" program predicts precise times and locations of crimes so that departments will allocate their officers accordingly.[13] In addition, law enforcement has deployed algorithms in the hopes of deterring criminal behaviors and warning community members of high-risk locations and times.[14]

Predictive policing is oriented towards surveillance rather than targeting individuals with particularized suspicion or making arrests.[15] Thus, the algorithms implicate few, if any, Fourth Amendment concerns. The algorithms are employed without targeting or

8. PERRY, ET AL., *supra* note 4, at 8; *id.* at 14.

9. Zarsky, *supra* note 5, at 1518.

10. Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, in HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY 21, 21–39 (Batya Friedman ed., 1997) (describing the influence of design decision in algorithms generally).

11. PERRY, ET AL., *supra* note 4, at 13 (exploring the importance of good data for predictive accuracy).

12. Joel Rubin, *Stopping Crime before It Starts*, L.A. TIMES (Aug. 21, 2010), http://articles.latimes.com/2010/aug/21/local/la-me-predictcrime-20100427-1 [https://perma.cc/R2KF-V5FD] (discussing the benefits of predictive policing in Los Angeles).

13. Spencer, *supra* note 7, at 505.

14. PERRY ET AL., *supra* note 4, at 2.

15. Spencer, *supra* note 7, at 494.

particularized suspicion.[16] Right now, the most common uses of the technology are predicting stranger offenses and organized crime,[17] although predictive policing has also been employed in other tasks, like predicting terrorist activity, city inspection services, and ranking tax returns for audits on the likelihood of tax evasion.[18] The technology predicts locations where crime is most likely to occur without reference to any individual or organization. In turn, this means the predictive technology alone does not form the basis for reasonable suspicion or probable cause. No search or seizure has occurred at the time of the prediction nor is made on account of that prediction. Because the Fourth Amendment is only implicated upon an unreasonable search or seizure, predictive policing technologies circumvent the Fourth Amendment.

High-tech predictive policing has already begun to take root in local law enforcement.[19] Departments are determining patrol routes and distributing officers throughout their jurisdictions on the basis of these predictions.[20] Although the most common types of predictions are location and time-based, Chicago has also used

16. Ferguson, *supra* note 6, at 287 (noting that there are "no reported cases on predictive policing in the Fourth Amendment context"). The Fourth Amendment comes into play after police officers have made an arrest or search and resolves around the rationale for that arrest. While predictive policing algorithms may facilitate eventual arrests, they are not yet used to provide the basis for arrests. Therefore, the use of such algorithms are not an aspect of the Fourth Amendment reasonable suspicion or probable cause inquiries.

17. PERRY ET AL., *supra* note 4, at 3 (discussing the use of predictive policing in stranger offenses); Scott Harris, *Product Feature: Predictive Policing Helps Law Enforcement "See around the Corners,"* POLICE CHIEF, http://www.policechiefmagazine.org/product-feature-predictive-policing-helps-law-enforcement-see-around-the-corners [https://perma.cc/3HNP-W6LB] (arguing that predictive policing best addresses organized criminal activity).

18. V.S. Subrahmanian, *Introducing the Software That Can Predict New Leaders of Terror Groups,* OBSERVER (London) (Sept. 15, 2013), http://www.theguardian.com/world/2013/sep/15/al-qaida-terrorist-leader [https://perma.cc/TZ33-WWFM] (discussing the use of predictive policing to combat terrorist activity); VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 7-8, 11-12, 15 (2013) (discussing the use of predictive policing for city inspections in New York City); ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 11 (2013) (discussing the use of predictive policing in IRS tax audits).

19. Andrew Papachristos, *Use of Data Can Stop Crime by Helping Potential Victims*, N.Y. TIMES, ROOM FOR DEBATE (Nov. 18, 2015, 10:13 AM), https://www.nytimes.com/roomfordebate/2015/11/18/can-predictive-policing-be-ethical-and-effective/use-of-data-can-stop-crime-by-helping-potential-victms [https://perma.cc/L6D4-7JP2] (discussing how predictive policing is being used in Chicago, Kansas City, Boston, New Orleans, and New Haven).

20. *See supra* nn. 17–18.

predictive policing to assign individuals a "score" representing their likelihood of becoming involved with a violent crime.[21] In a city of 2.7 million, Chicago police have identified the 1,400 people most at risk and joined forces with social workers for "interventions" in the hope of helping them avoid crime.[22] There is little evidence to-date of widespread adoption of Chicago's use for predictive technologies.[23]

B. Benefits of Predictive Policing

By improving the accuracy of estimates of where and when crimes will occur, predictive policing can make departments more effective and efficient.[24] The algorithms are also cheaper than increasing police force sizes, and they cut back on the amount of unnecessary harassment people face in the street, as I explain further below.[25] At least in theory, predictive policing is an alternative to "flawed investigative tools" that leads to safer streets at a lower economic cost and a lower social cost.[26]

Beyond the attempt to reduce unnecessary surveillance actions, predictive policing seeks to reduce the social costs of policing in three other ways. Policing in America has always been a contentious issue that cannot be entirely understood without reference to

---

21. *See* Jeremy Gorner, *Chicago Police Use 'Heat List' as Strategy to Prevent Violence*, CHI. TRIB. (Aug. 21, 2013), http://articles.chicagotribune.com/2013-08-21/news/ct-met-heatlist20130821_1_chicago-police-commander-andrew-papachristos-heat-list/ [http://perma.cc/H5MB-JKKF] (discussing the Chicago "heat list").

22. Monica Davey, *Chicago Police Try to Predict Who May Shoot or Be Shot*, N.Y. TIMES (May 23, 2016), https://www.nytimes.com/2016/05/24/us/armed-with-data-chicago-police-try-to-predict-who-may-shoot-or-be-shot.html?_r=1 [https://perma.cc/KP5E-T4FC]. I discuss the concern these "interventions" may be pretext later in this Note.

23. Beth Pearsall, *supra* note 3, at 17 (2014) (specifying predictive policing's use in "analytic tools and techniques like hot spots, data mining, crime mapping, geospatial prediction and social network analysis . . .").

24. M. Todd Henderson, Justin Wolfers, & Eric Zitzewitz, *Predicting Crime*, 52 ARIZ. L. REV. 15, 34–38 (2010). The ability of predictive policing to actually reduce crime is itself still uncertain. One recent study found that a predictive policing program was not able to significantly reduce property crime. PRISCILLIA HUNT, JESSICA SAUNDERS, & JOHN S. HOLLYWOOD, EVALUATION OF THE SHREVEPORT PREDICTIVE POLICING EXPERIMENT 49 (2014). It did, however, reduce costs by 6–10%, and the negative results were specific to one program, not predictive technologies generally. *Id.* at 47, 49–50.

25. Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 224 (2015).

26. Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 28–30 (2016) (discussing each alternative to predictive policing in turn).

its racialized history.[27] In the last several years, this issue has come to a head with the widely publicized deaths of Black men and the rise of the Black Lives Matter movement.[28] Predictive policing provides a basis for the distribution of policing resources that curtails police discretion, which has been identified as one of the root causes of biased policing.[29] In general, policing also sweeps in more individuals than it should with unnecessary intrusions and physical invasions. Any time an officer stops, questions, or searches an individual or their possessions there is a cost in time, humiliation, autonomy, and dignity to that individual.[30] Stops, questionings, and searches that prove unfruitful also impose that same harassment cost but without any law enforcement benefit to show for it.[31] Predictive policing theoretically minimizes those costs by avoiding unnecessary encounters. The production of data also facilitates audits and third-party reviews of police departments,[32] lending legitimacy to law enforcement and providing a means to improve existing policies.

No one is arguing that predictive policing is the solution to all challenges in American law enforcement, but supporters contend that predictive algorithms, along with other tools, can make policing more effective, efficient, legitimate, and fair.

---

27. *See generally* Cassandra Chaney & Ray V. Robertson, *Racism and Police Brutality in America*, 17 J. OF AFR. AM. STUD. 480 (2013) (providing an overview of racism in policing over the last several decades).

28. I acknowledge this has been a publicized issue for decades and also recognize the success of the efforts of Alicia Garza and her co-activists in reinvigorating public discussion on the issue. *About*, BLACK LIVES MATTER (Mar. 11, 2017), http://blacklivesmatter.com/about [https://perma.cc/TX63-QUC3] (summarizing the national movement's rise after several widely publicized deaths).

29. PHILLIP A. GOFF ET. AL., URBAN INST., THE SCIENCE OF POLICING EQUITY: MEASURING FAIRNESS IN THE AUSTIN POLICE DEPARTMENT 14 (2016) (using quantitative analysis to conclude discretion increased racially biased outcomes). Of course, explicit racism also plays a large role in racist outcomes.

30. *See* Bambauer, *supra* note 25.

31. I recognize some in law enforcement communities would argue that even an unsuccessful law enforcement encounter helps to maintain a feeling of safety and deter crimes. Even if one supports this method of law enforcement, I think all would still acknowledge there is less benefit to an officer action that interferes with innocent activity.

32. Joh, *supra* note 26, at 29.

C. Hazards of Predictive Policing[33]

Government surveillance has unsettled Americans since the founding of our country,[34] and the modern rise of big data-fueled predictions in the commercial context has further unnerved American consumers.[35] Using big data techniques from the private sector to refine government surveillance risks popular discontent. Any level of surveillance is to some degree inherently intrusive.[36] Surveillance requires increased attention on individuals, prying into our private matters, and, in many cases, stops and/or searches. Popular understanding of predictive policing framed by science fiction,[37] along with legitimate concerns about misappropriation of data and predictions,[38] could harm communities' relationships with and trust in the police.[39]

Another concern with predictive policing is that the algorithms will fail to correct grievances over policing while giving departments and politicians the grounds to declare "mission accomplished."[40] Because predictive algorithms rely on preexisting data, biased data can generate biased predictions.[41] For example, if drug arrests in a

33. I start by comparing the costs and benefits of predictive policing to provide a framework for considering transparency needs, but in so doing, do not mean to suggest the question of whether to use predictive policing can be resolved through a simple cost-benefit analysis. Assuming cost-benefit analysis could resolve this issue ignores the fact that many of the hazards of predictive policing I discuss in this section, particularly discriminatory ones, should be treated as hard stops to any new policing techniques.

34. *See* U.S. CONST. amend. IV.

35. *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant before her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#391d1db66686 [https://perma.cc/TE5C-EKYU]; Charles Duhigg, *How Companies Learn your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/S9QW-W56F].

36. Bambauer, *supra* note 25.

37. *See, e.g.*, MINORITY REPORT (DreamWorks 2002).

38. *See* Evan Perez, *NSA: Some Used Spying Power to Snoop on Lovers*, CNN (Sept. 27, 2013), http://www.cnn.com/2013/09/27/politics/nsa-snooping [https://perma.cc/3UBU-7SEC].

39. PERRY ET AL., *supra* note 4, at 81–83.

40. *Cf.* Adam M. Samaha, *Regulation for the Sake of Appearance*, 125 HARV. L. REV. 1563, 1620–33 (2012) (arguing that the appearance of success with broken windows policing allows police to continue with the practice even if the broken windows strategy does not work in actuality).

41. Sarah Brayne, Stratified Surveillance: Policing in the Age of Big Data (2015) (unpublished Ph.D. dissertation, Princeton University) (on file with Mudd Manuscript Library, Princeton University). Of particular concern is the role algorithms might play in "amplify[ing] feedback problems" because of the use of prior outputs to shape future inputs. Matt Reynolds, *Biased Policing is Made Worse by Errors*

community have previously skewed towards a particular racial group, then a prediction of future drug crimes based on that data will also skew towards that community. The complexity of algorithms also makes these biases harder to identify and remove because fixing the problem requires some understanding of the algorithm or computer code itself.[42] An algorithm may further conceal the issue by not directly relying on race but instead incorporating race as a factor through correlated variables.[43] The *appearance* of a "neutral mechanism" knocks the wind out of the sails of social justice movements working to redress these wrongs. Police departments can respond to such movements by claiming they have already instituted the desired change, even while that change proves hollow in reality.

Even assuming algorithms are accurate and unbiased, some fear that police will not rely on the algorithms.[44] Beyond wasting the resources invested in these algorithms, activists fear predictive policing will mask policing issues and become an impotent alternative to meaningful proposals.[45]

D. How Law Enforcement Obtains the Technology

Given the technology's sophistication, law enforcement typically purchases predictive policing algorithms from outside contrac-

---

in Pre-Crime Algorithms, NEWSCIENTIST (Oct. 4, 2017), https://www.newscientist.com/article/mg23631464-300-biased-policing-is-made-worse-by-errors-in-pre-crime-algorithms [https://perma.cc/ZE6R-VNHV]; *see also* Danielle Ensign et. al, *Runaway Feedback Loops in Predictive Policing*, PROCEEDINGS OF MACHINE LEARNING RESEARCH 81:1–12 at 8–10 (2018), http://proceedings.mlr.press/v81/ensign18a/ensign18a.pdf [https://perma.cc/N2HR-98V6] (using Predpol to study runaway feedback problems with predictive policing).

42. Jens Ludwig, Director, Uni. of Chi. Crime Lab, Keynote Address at the Policing and Accountability in the Digital Age Conference (Sep. 15, 2016); Michael L. Rich, *Machines as Crime Fighters*, 30-WTR CRIM. JUST. 10, 13 (2016).

43. Anna M. Barry-Jester, Ben Casselman, & Dana Goldstein, *Should Prison Sentences Be Based on Crimes that Haven't Been Committed Yet?*, FIVETHIRTYEIGHT (Aug. 4, 2015), https://fivethirtyeight.com/features/prison-reform-risk-assessment [https://perma.cc/DL95-W9U2].

44. Henderson, Wolfers, & Zitzewitz, *supra* note 24, at 23 (expressing concern that predictions may "be lost in the noise of the station house").

45. Kami C. Simmons, *Police Technology Shouldn't Replace Community Resources*, N.Y. TIMES, ROOM FOR DEBATE (Nov. 18, 2015, 3:22 AM), http://www.nytimes.com/roomfordebate/2015/11/18/can-predictive-policing-be-ethical-and-effective/police-technology-shouldnt-replace-community-resources [https://perma.cc/7VWW-XAB3] (arguing predictive algorithms fail to account for soft factors that are not in the algorithm and are a poor replacement for community policing); Joh, *supra* note 26, at 32 (arguing predictive algorithms eliminate good discretion that officers may gain from personal and community relationships).

tors rather than developing the algorithms themselves.[46] A number of companies have already profited from selling predictive algorithms to the government with varying purposes and levels of sophistication.[47] Some of these companies provide substantial support so that departments better understand the capabilities and limitations of the technology, as well as best practices for incorporating the predictions into existing department schemes. Other companies focus more exclusively on development and sales, leaving the practical implementation of the algorithms to law enforcement departments.[48] Either way, it is clear that the private sector has been at the forefront of developing this technology.[49]

But the involvement of private actors complicates the hazards of predictive policing. Separating development from implementation is sheltering the algorithm from public review, which amplifies concerns about noisy data, improper biases, and flawed algorithms.[50] The intellectual property rights of private companies add a layer of secrecy to predictive policing. Private developers who do not wish to relinquish information to the public can hide behind proprietary rights, which raises accountability concerns. Whose job is it to ensure models are working correctly? Who do we hold liable when things go wrong? Do we blame the developer or the user? When fingers point in both directions, it creates an accountability gap. The combination of high-tech surveillance and private development necessitates comprehensive transparency.

46. *See, e.g.*, PREDPOL, http://www.predpol.com (providing an example of a private company's product); *see also* Cynthia Rudin, *Predictive Policing: Using Machine Learning to Detect Patterns of Crime*, WIRED (Aug. 2013), https://www.wired.com/insights/2013/08/predictive-policing-using-machine-learning-to-detect-patterns-of-crime [https://perma.cc/XN38-FK9K] (giving an example of collaboration with a private university).

47. *See, e.g., id.*; *IBM100 - Predictive Crime Fighting*, IBM100, http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/crimefighting [https://perma.cc/LNX7-MBVS] (describing IBM's products like Blue Crush); HUBSPOT, https://www.hubspot.com [https://perma.cc/EN2X-ZNFY]; PALANTIR, http://www.palantir.com/solutions/law-enforcement [https://perma.cc/8ZEP-LFQK].

48. PERRY ET AL., *supra* note 4, at 126–27 (arguing developers should provide more decision support for resource allocation and continuing assistance to departments that purchase their technology).

49. *See supra* Part I.b.

50. PERRY ET AL., *supra* note 4, at 89 (outlining the problem of "noisy and conflicting data").

II.
TRANSPARENCY: THE CURRENT ARGUMENTS

A. Routes to Information

Oversight requires some degree of transparency and, in the case of predictive policing, that transparency should be oriented towards the general public. The question of to *whom* should predictive practices be transparent antecedes the question of *how* should that transparency be achieved. If private developers and local law enforcement currently hold the keys to that vault of information, the question becomes whether transparency is better achieved by handing those keys to another or by simply leaving the vault open for any curious passerby. Several institutions could be tasked with the responsibility of overseeing predictive policing: law enforcement, courts, legislatures, or civilian review boards. However, flaws with each of these institutions leaves public oversight as the best option.

Law enforcement has institutions designed for oversight and review.[51] However, self-regulation within law enforcement comes with years of baggage, including the code of silence, conflicts of interest, and a perceived lack of objectivity.[52] Data-collection-based technologies have exacerbated these challenges with added complexity often poorly understood by local law enforcement users.[53]

---

51. *See* 34 U.S.C. § 12601 (2018) (giving the DOJ Civil Rights Division authority to bring suits against local police departments). *See generally* N.Y.C. Comm'n To Combat Police Corruption, Performance Study: A Fellow-Up Review Of The IAB's Command Center (Aug. 1999), https://www1.nyc.gov/assets/ccpc/downloads/pdf/Performance-Study-A-Follow-up-Review-of-the-Internal-Affairs-Bureau-Command-Center-August-1999.pdf [https://perma.cc/2UTE-FNKG] (summarizing the NYPD's Internal Affairs Bureau).

52. Steven D. Seybold, *Somebody's Watching Me: Civilian Oversight of Data-Collection Technologies*, 93 Tex. L. Rev. 1029 (2015), 1041–42 (summarizing the weaknesses of self-regulation); Dina Mishra, *Undermining Excessive Privacy for Police: Citizen Tape Recording to Check Police Officer's Power*, 117 Yale L.J. 1549, 1552 (2008) ("Policy corruption can undermine internal monitoring and sanctions even where they do apply."). Police departments face a challenge in self-regulation. Culture and the desire to stand together makes it difficult for whistleblowers to report colleagues and superiors. This challenge has led many to advocate for civilian review boards and similar external checks on departments.

53. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 4, 7–9 (2008) (tracing the growth of private-public coordination in security technology); Justin Jouvenal, *Police Are Using Software to Predict Crime. Is It the 'Holy Grail' or Biased Against Minorities?*, Wash. Post (Nov. 17, 2016), https://www.washingtonpost.com/local/public-safety/police-are-using-software-to-predict-crime-is-it-a-holy-grail-or-biased-against-minorities/2016/11/17/525a6649-0472-440a-aae1-b283aa8e5de8_story.html [https://perma.cc/E5FB-XQSF] (discussing

Courts, the traditional oversight mechanism for much of law enforcement's activities,[54] are an especially weak check on predictive policing because they are limited by constitutional law in how they may restrain law enforcement. The Fourth Amendment's protections apply only after there is an invasion of a reasonable expectation of privacy.[55] Because predictive policing is used for surveillance, which does not require reasonable suspicion, police can observe citizens without any court interference.[56] Courts may never consider predictive policing policies if no relevant case is ever brought.

Legislatures, on the other hand, face political pressure. As Professor Donald Dripps explains, legislatures face political pressures to adopt the strongest law enforcement policy rather than the fairest or most reasonable policy.[57] Driven by elections, legislators fear the perception of public safety cut-backs and are hard-pressed to craft rules that limit law enforcement resources.

In addition to procedural and political challenges, both courts and legislatures face another problem in making any information they learn public. DOJ and internal police reviews have worked to conceal technologies from the public, using devices such as non-

---

law enforcement's incomplete understanding of how predictive policing technology works).

54. Stephen D. Mastrofski & James J. Willis, *Police Organization Continuity and Change: Into the Twenty-First Century*, 39 CRIME & JUST. 55, 115 (2010) ("Courts oversee a range of police practices: personnel and administrative matters, as well as practices in the field.").

55. *See* Katz v. United States, 389 U.S. 347 (1967). *See generally* William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 780 (2006) (arguing reliance on Constitutional law has hampered attempts to remedy problems in criminal justice).

56. Seybold, *supra* note 52, at 1044–45 (describing the weakness of judicial oversight). Judicial oversight is especially weak when it comes to the surveillance of individuals in public places, even when that oversight relies upon technology; United States v. Steinhorn, 739 F. Supp. 268, 272 (D. Md. 1990) (citing United States v. Batchelder, 442 U.S. 114, 124 (1979)) (holding law enforcement does not need reasonable suspicion to observe and investigate persons' public conduct).

57. Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; or Why Don't Legislatures Give a Damn about the Rights of the Accused*, 44 SYRACUSE L. REV. 1079, 1080 (1993) (using public choice theory to explain why reliance on legislatures to constrain law enforcement will prove futile). Legislatures are also easier to buy, as evidenced by PredPol's $2 million dedicated to lobbying the Arizona statehouse. Ali Winston & Ingrid Burrington, *A Pioneer in Predictive Policing is Starting a Troubling New Project*, VERGE (Apr. 26, 2018, 1:36 PM), https://www.theverge.com/2018/4/26/17285058/predictive-policing-predpol-pentagon-ai-racial-bias [https://perma.cc/44ZW-4PPV].

disclosure agreements to avoid challenges to their practices.[58] Courts often review technologies *in camera*, and, in general, American courts are opaque with little public scrutiny.[59] Thus, these institutions prove fairly weak at distributing information to the public.[60] Opening up information to the public avoids these transparency hurdles, helps to ensure meaningful oversight, and furthers several normative goals that I discuss below.

B. Arguments for Transparency

Previous advocates for transparency have offered variations on five arguments: (1) democratic legitimacy, (2) the prevention of misconduct, (3) a remedy for injustices, (4) better substantive policies, and (5) community trust.

First, transparency lends democracy legitimacy. Transparency has inherent value: openness in government has been a stalwart companion to democracy, as it creates the well-informed public necessary to sustain democracy.[61] The Freedom of Information Act (FOIA) and its state counterparts recognize the basic right of American citizens to obtain government information,[62] and many argue that the necessity of an informed citizenry for popular sovereignty

58. Aff. of FBI Supervisory Special Agent Bradley S. Morrison, Chief, Tracking Technology Unit, Operation Technology Division in Quantico, Virginia, at 2, Apr. 11, 2014, attach. to City's Verified Answer, Hodai v. City of Tucson, No. C20141225 (Ariz. Super. Ct. Apr. 14, 2014).

59. Stephanos Bibas, Essay, *Transparency and Participation in Criminal Procedure*, 81 N.Y.U. L. REV. 911, 920–31 (2006) (discussing the exclusion of outsiders from judicial proceedings).

60. There is an argument for enlisting civilian review boards as the means of obtaining and distributing information with predictive policing. I do not focus on it here because many existing constraints and normative arguments that apply to civilian review boards would also apply to transparency with the general public. In addition, the boards have yet to catch on and become popular in the United States. Udi Ofer, *Getting It Right: Building Effective Civilian Review Boards to Oversee Police*, 46 SETON HALL L. REV. 1033, 1053 (2016) (only six of the fifty largest police departments currently have civilian review boards with any serious authority). For an argument in favor of civilian review boards, *see id.*

61. Scherr v. Universal Match Corp., 297 F. Supp. 107, 110 (S.D.N.Y. 1967) (quoting 12 ASCAP Copyright Law Symposium 96, 105 (1961)); Jeremy Bentham, An Essay on Political Tactics (1791), *reprinted in* 2 THE WORKS OF JEREMY BENTHAM, 299, 310–12 (John Bowring ed., Russell & Russell 1962) (1843) ("To conceal from the public the conduct of its representatives, is to add inconsistency to prevarication . . . .").

62. 5 Ill. Comp. Stat. 140/1 (2006) (". . . all persons are entitled to full and complete information regarding the affairs of government . . . ."); Sullo & Bobbitt, PLLC v. Abbott, 2012 WL 2796794 (N.D. Tex. 2012) (working under the assumption there is no absolute right to information held by the government).

trumps personal privacy rights.[63] As the Republic rules only with the consent of the governed, the governed must be informed of the Republic's material activities in order to agree to its rule.[64]

Second, transparency aids accountability, preventing police misconduct.[65] An informed citizenry is able to check against corruption and "protect the public from secret government activity."[66] Unlike my first argument, this is a monitoring claim rather than a social contracting claim. While evidence of wrongdoing is not a prerequisite to disclosure,[67] transparency helps to prevent and redress police abuses of power. Electoral incentives can lead politicians to make popular but ineffective decisions.[68] Transparency gives the public the ability to check the work of the political branches rather than relying on government officials to self-report. Just as transparency has changed policies in the past, such as restricting the use of the controversial Stingray technology,[69] transparency could revise predictive policing policies, as well.

Third, when misconduct does occur, whether with law enforcement policies or predictive policing, transparency helps provide a remedy to the aggrieved party. Part of the role of adjudicatory bodies is to provide legal and public recognition that a wrong has occurred.[70] That recognition provides some relief to the aggrieved

63. *See, e.g.*, Jesse H. Alderman, *Police Privacy in the iPhone Era?: The Need for Safeguards in State Wiretapping Statutes to Preserve the Civilian's Right to Record Public Police Activity*, 9 First. Amend. L. Rev. 487, 523 (2011).

64. Barry Friedman, *Secret Policing*, 2016 U. Chi. Legal F. 99, 120 (2016) (". . . the members of the public — the electorate are their bosses. And the bosses have a right to know what is going on.").

65. Adam M. Samaha, *Government Secrecy, Constitutional Law, and Platforms for Judicial Intervention*, 53 UCLA L. Rev. 909, 970 (2006) ("Popular accountability depends on information access . . . .").

66. Lambries v. Saluda Cty. Council, 409 S.C. 1, 15 (2014); *see also* Elkins v. Federal Aviation Admin., 99 F. Supp. 3d. 90, 95 (D.D.C. 2015) ("The basic purpose of FOIA is to ensure an informed citizenry . . . needed to check against corruption and to hold the governors accountable to the governed." (quoting John Doe Agency v. John Doe Corp., 493 U.S. 146, 152 (1989))).

67. *E.g.,* Chicago All. for Neighborhood Safety v. City of Chicago, 808 N.E.2d 56, 73 (Ill. App. Ct. 2004) (holding plaintiffs need not show illegal or unethical conduct to prevail in an Open Records suit for information regarding police activities).

68. *See* Dripps, *supra* note 57, at 1089 (describing the weaknesses of legislative oversight of law enforcement).

69. H. 4522, 121st Leg. (S.C. 2015).

70. The concept of moral signaling to build social cohesion has deep roots in criminal jurisprudence. *See generally* H.L.A. Hart, *Social Solidarity and the Enforcement of Morality*, 35 U. Chi. L. Rev. 1 (1967); Emile Durkheim, Social Cohesion and Anomie (1895).

and helps demarcate the boundaries of acceptable behavior.[71] Transparency with predictive policing allows the public to ensure law enforcement recognizes any wrongful uses of predictive policing against aggrieved individuals and communities. It also helps inform what is an acceptable use of predictive policing.

Fourth, transparency produces better policies. Much of this argument boils down to the age-old idea that two heads are better than one. Transparency allows a greater number of parties, with a greater variety of interests, to review predictive policing. The public includes organizations devoted to analysis that can give more attention to issues than law enforcement.[72] As previously discussed, mechanization often carries with it hidden subjectivities and errors creating biases in application.[73] The Breathalyzer, for example, was a black box not fully understood by many in law enforcement. Widespread "public acceptance and cultural prestige" delayed in-depth analysis of its flaws for several decades, and now the certainty of criminal sentences has come under doubt.[74] Similarly, widespread acceptance of predictive policing could risk faults lying undetected for years. Transparency ameliorates that problem by allowing scrutiny early in the process, catching flaws before adoption rather than decades after. The crowdsourcing of predictive policing review is especially important because its complexity requires expertise, time, and attention, which non-governmental organizations can provide.[75]

Fifth, transparency builds community trust. This argument can cut two ways. Revelations of furtive predictive policing could outrage citizens in the same way revelations of the furtive use of Sting-

71. *Cf.* Jenia I. Turner, *Policing International Prosecutors*, 45 N.Y.U. J. INT'L L. & POL. 175, 205–07, 212 (2012) (making this argument in the context of international prosecutions).

72. *See* ELIZABETH T. BORIS, NONPROFIT ORGANIZATIONS IN A DEMOCRACY – ROLES AND RESPONSIBILITIES, 41–46 (2006).

73. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 10–16 (2014); Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 676 (2010).

74. Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1260–76 (2016); Reginald Fields, *Ohio Commits $6.4 Million For New Breathalyzers That Face Lawsuits Across The Country*, CLEVELAND PLAIN DEALER (Nov. 17, 2008), http://blog.cleveland.com/metro/2008/11/ohio_commits_64_million_for_ne.html [https://perma.cc/LE6P-DLQW]; *Lawyers: Massachusetts Withheld Evidence About Breathalyzers*, INS. J. (Aug. 28 2017), https://www.insurancejournal.com/news/east/2017/08/28/462537.htm [https://perma.cc/E9BV-QA3T].

75. BORIS, *supra* note 72, at 41–46.

rays did.[76] What citizens do not know, they cannot get mad about.[77] On the other hand, transparency may increase community trust in the long run. The refusal to answer requests for public inspection diminishes public trust.[78] Transparency gives the public answers and ensures law enforcement provides information upfront. When reporters broke stories about Stingrays, public trust took a serious hit, not just because of the use of the technology, but because law enforcement hid the technology from the public.[79] Assuming an agency's use of predictive policing will eventually come to light, it is better for public trust for law enforcement, rather than journalists, tabloids, and blogs, to break the story.

III.
ADDITIONAL ARGUMENTS FOR TRANSPARENCY SPECIFIC TO PREDICTIVE POLICING

I add three arguments to make the case for transparency with predictive policing: transparency (1) provides a democratic check where democratic oversight is particularly weak, (2) aids the effectiveness of predictive policing through deterring crime, and (3) cuts down on an unfair distribution of costs.

A. Transparency as an Additional Deterrent

Transparency with predictive policing deters criminal activity by increasing trust in the system of law enforcement and notifying the public of improved law enforcement techniques.

1. Improved Effectiveness through Broader Trust in Law Enforcement

Forty-eight percent of the public lacks confidence in police.[80] Many feel themselves on the wrong side of a gulf separating insiders and outsiders of the system. Those on the outside feel they are unfairly targeted through discriminatory law enforcement practices and have no say in their design.[81] Much of the discontent with po-

76. Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance [https://perma.cc/PY58-ZMFX].

77. Of course, that Orwellian argument sacrifices democratic legitimacy.

78. Steven D. Zansberg & Pamela Campos, *Sunshine on the Thin Blue Line: Public Access to Police Internal Affairs Files*, 22 COMM. LAW. 34, 34 (2004).

79. *See* Reel, *supra* note 76.

80. Jeffrey M. Jones, *In U.S., Confidence in Police Lowest in 22 Years*, GALLUP (Jun. 19, 2015), http://www.gallup.com/poll/183704/confidence-police-lowest-years.aspx (finding a 52% confidence in police – the lowest since 1993).

81. *See* BLACK LIVES MATTER, *supra* note 28.

licing today does not come from substantive law but from procedural injustices.[82] An individual who believes he is stopped by an officer because he is speeding has a much more positive view of law enforcement, as well as greater trust in officers, than an individual who believes he is stopped by an officer on account of his race or religion.[83]

Those who believe in the fairness of procedures are more likely to obey police commands and laws even when authorities are not present.[84] Tom R. Tyler, a professor of psychology and law at Yale University, has led much of this research, finding a correlation between those who believe the legal system is fair and those who obey the law.[85] Tyler's research suggests that most people comply with the law not for fear of getting caught, but out of a belief that the law and legal system are legitimate.[86] Personal experiences with the law and media stories shape that sense of legitimacy,[87] so positive experiences and stories help to build a self-regulating society. Fewer laws are broken when people appreciate the system behind those laws.

This is where the argument regarding predictive policing's ability to build community trust in law enforcement comes into play. Transparency builds trust by giving the public answers and avoiding media scandals.[88] Transparency also allows the public to play an active role in shaping policy, promoting buy-in from communities affected by those policies.[89] Combatting disparate attention from law enforcement, predictive policing provides a reasoned, numerical method for distributing law enforcement resources.[90] While concerns about racial bias continue with predictive

82. *See* Tom R. Tyler et al., *Street Stops and Police Legitimacy: Teachable Moments in Young Urban Men's Legal Socialization*, 11 J. EMPIRICAL LEGAL STUD. 751 (2014).

83. Tom R. Tyler, *Procedural Justice, Legitimacy, and the Effective Rule of Law*, 30 CRIME & JUST. 283, 329 (2003) (analyzing through psychology).

84. *Id.* at 284.

85. TOM R. TYLER, WHY PEOPLE OBEY THE LAW 4–5 (1990). Professor Tyler first popularized the theory that the legitimacy of the legal system could benefit compliance with the law, and upon additional testing has found a moderately strong correlation between faith in the legal system and obedience to the law. *E.g.*, Tom R. Tyler & Jeffrey Fagan, *Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities?* 6 OH. ST. J. CRIM. L. 231, 246 (2008) (finding a correlation over .5 for obligation, trust, confidence in the legal system (indices for legitimacy) and identification with the police).

86. *Id.* at 178.

87. *Id.*

88. Zansberg & Campos, *supra* note 78, at 34.

89. Reel, *supra* note 76.

90. *See* BLACK LIVES MATTER, *supra* note 28.

algorithms because algorithms incorporate preexisting data that may be biased, ex ante transparency can help to resolve those concerns. Outside actors can review algorithms to identify problems like racial bias and propose effective solutions. At the very least, a willing commitment to transparency and active effort to improve policy should encourage greater trust in and legitimization of law enforcement. This trust and legitimacy will in turn further the ultimate law enforcement goal of increasing compliance with the law.

2. Improved Effectiveness through a Deterrence Effect

Throughout this article, I have assumed that predictive policing works at least to some degree. Assume for a moment that it does not work—that police officers could get just as much out of rolling dice. Even then, transparent predictive policing still provides a social benefit—deterrence.

In 2013, the Memphis Police Department found itself relying on luck when its predictive policing proved to be ineffective.[91] Memphis had relied upon results from the Blue Crush system for over three years to allocate resources throughout the city and determine when officers should assume their posts. Three years after implementing the system, crime had decreased thirty percent in the metropolitan area, and the department had repeatedly publically attributed the improvement to Blue Crush.[92]

A system audit, however, soon revealed that "reams of data" had not been input into the system. Without that data, the system could not accurately predict where crimes were going to occur.[93] The police may as well have been rolling dice, but the department's effectiveness had substantially improved. How could this have happened? The answer could rest in the web of social factors that influences crime rates and continues to elude most scholars on the topic.[94] The better answer is that appearance shapes reality.[95]

---

91. Leslie A. Gordon, *A Byte Out of Crime*, A.B.A J., Sept. 2013, at 18, 19.

92. *See* Andrew Ashby, *Operation Blue C.R.U.S.H. Advances at MPD*, MEMPHIS DAILY NEWS (Apr. 7, 2006), https://www.memphisdailynews.com/editorial/Article.aspx?id=30029 [https://perma.cc/UQ8Q-YXVC]; *Blue Crush Statistics*, WMCACTIONNEWS5, http://www.wmcactionnews5.com/story/4924493/blue-crush-statistics; *Memphis Police Department Reduces Crime Rates with IBM Predictive Analytics Software*, IBM NEWS ROOM (Jul. 21, 2010), https://www-03.ibm.com/press/us/en/pressrelease/32169.wss [https://perma.cc/RB4B-BZJD].

93. Gordon, *supra* note 91.

94. Peter-Jan Engelen, et al., *What Determines Crime Rates? An Empirical Test of Integrated Economic and Sociological Theories of Criminal Behavior*, 53 THE SOC. SCI. J. 247 (2016) (noting the uncertainty of which factors are related to crime rates and adding their own quantitative analysis to the mix).

For example, the appearance of a weak fiscal state at a bank creates a bank run, which in turn brings that weak fiscal state to fruition.[96] Whether or not the bank was in actuality weak to begin with is of little importance. What matters for the end result is the *appearance* of instability, and even a false or illogical belief can impose such results.[97] Applied to predictive policing, the appearance of a predictive algorithm in Memphis may have helped reduce crime. The Memphis community was aware of the algorithm, believed in its ability to predict where crime was likely to occur, and became convinced police would foil criminal plots. Community members chose not to attempt crime in the first place, and the crime rate fell.[98] While many obey the law out of the perceived legitimacy of the law alone, for those weighing the likelihood of getting caught, better policing tools matter.[99]

The influence of public perceptions can augment the decrease in crime resulting from predictive policing. Of course, a properly applied algorithm would have benefitted Memphis more than one with missing inputs. I am not arguing that the effectiveness of the algorithm is irrelevant, but instead that transparency—sharing with the public the fact that a predictive policing algorithm is in use—has substantial benefits for law enforcement. The LAPD has instituted audits of its own Blue Crush system.[100] Transparency with the LAPD system and the audit furthers the deterrence mission of the department.[101] Moreover, transparency decreases crime without putting citizens or police officers in harm's way. This argument does not address what aspect of the predictive algorithm should be released, and the argument that certain information could be used by criminals to avoid law enforcement persists. Regardless, transparency provides an opportunity to avoid the tremendous social

95. Samaha, *supra* note 40, at 1582–97 (2012) (discussing the relationship between appearance and reality).

96. *Id.* at 1592–96 (providing the example of a bank run).

97. Robert K. Merton, *The Self-Fulfilling Prophecy*, 8 ANTIOCH REV. 193, 195 (1948) (discussing the superficial importance of truth or logic to beliefs for results).

98. *See supra* note 96.

99. Tyler, *supra* note 83, at 329.

100. Guy Adams, *The Sci-Fi Solution to Real Crime*, INDEPENDENT (Jan. 11, 2012), https://www.independent.co.uk/news/world/americas/lapds-sci-fi-solution-to-real-crime-6287800.html [https://perma.cc/W3DX-EBHQ] (describing the LAPD's double-blind testing of its technologies to prevent flawed data).

101. An audit is one means of publicizing the fact that predictive policing is in place. This makes the community more aware of the policing tool, which can deter crime. *See supra* nn. 95–99.

costs of intervening in suspected criminal affairs, because officers can rely upon the deterrent effect of predictive policing.

B. Transparency as an Accountability Gap-Filler

Predictive policing escalates challenges with accountability because it lacks a good democratic check. Without public transparency, errors are likely to go on undetected. Just like the fear of undetected flaws was at play with the Breathalyzer,[102] flaws in predictive policing have also raised concerns, especially the incorporation of old biases or flawed data.[103] Normally, law enforcement, legislatures, and courts would provide the democratic check ensuring the technology works as promised. As discussed above, these institutions prove especially ineffective in the context of predictive policing, as the technology is designed by an entity different from the one implementing it.[104]

Law enforcement lacks the resources to understand predictive algorithms and hold private developers accountable. Private companies develop predictive algorithms because they have the resources to develop the technology.[105] This means law enforcement never develops the same understanding of the algorithms as the private companies. This disparity in knowledge leaves law enforcement at the whims of analysts who have considerable discretion in algorithm design.[106] A single actor within law enforcement could in theory become an expert on a predictive algorithm, but, given the market fragmentation for predictive policing, expertise on every algorithm in use by law enforcement is likely unobtainable and unaffordable.[107] Law enforcement would either have to expend considerable resources hiring experts or grant one private developer a monopoly over the market. Of the many predictive technology options available, picking just one, or a few, is unlikely to satisfy the needs of departments across widely ranging communities. Either option impairs the expected benefits of predictive policing.

Courts could theoretically provide a platform for expert testimony and transparency, but courts will rarely encounter this de-

102. Roth, *supra* note 74, at 1260–72.

103. Brayne, *supra* note 41.

104. *See supra* Part II.a for a discussion of why other institutions would prove ineffective.

105. PredPol, *supra* note 46; Rudin, *supra* note 46.

106. Zarsky, *supra* note 5, at 1518.

107. *See* Miriam A. Cherry & Robert L. Rogers, *Markets for Markets: Origins and Subjects of Information Markets*, 58 Rutgers L. Rev. 339, 342 (2006) (discussing the fragmentation of the market).

bate. Unlike the Breathalyzer, which provides probable cause for arrests, predictive policing algorithms are just a means of distributing surveillance resources throughout a community. They do not provide probable cause or even reasonable suspicion.[108] There is no invasion of reasonable expectations of privacy to provide grounds for a suit in court. The delayed realization of concerns with the Breathalyzer provided an imperfect solution. Tiptoeing around the jurisdiction of the court, the situation with predictive policing delayed further.

The resulting lack of democratic oversight is more than just a problem of erroneous results.[109] We give a unique power to law enforcement to exert considerable force against us and engage in activities that would often be unlawful if carried out by a private citizen.[110] In the context of predictive policing, the government is delegating that power to algorithm developers. The information disparity between law enforcement and developers results in an *unchecked* delegation of democratically granted authority to a private party.

Public transparency resolves this issue by providing a check on developers. Transparency allows private parties who have greater expertise and resources to better inform the public by analyzing algorithms, their implementation, and their effects on communities.[111] Building on previous notions of the "private attorney general,"[112] these private parties can fill the information gap—educating both the public and public officials.

---

108. Seybold, *supra* note 52, at 1044–45. *But see* Ferguson, *supra* note 6 at 262 (2012) (suggesting predictive policing has Fourth Amendment ramifications). Courts will see FOIA suits, but the debate in those suits is over whether the suing party may gain access to predictive policing information. Before that information has been released to the public, there is no one with expertise in the area to evaluate the technology. The judge may review the information in camera, but a judge's in camera evaluation of predictive policing practically cannot be as thorough or scientific as external review by a testifying expert.

109. Barry Friedman, Unwarranted: Policing without Permission 5–6 (2017).

110. *Id.*

111. Boris, *supra* note 72, at 41–46.

112. *See generally* Myriam E. Gilles, *Reinventing Structural Reform Litigation: Deputizing Private Citizens in the Enforcement of Civil Rights*, 100 Colum. L. Rev. 1384 (2000); Carl Cheng, *Important Rights and the Private Attorney General Doctrine*, 73 Cal. L. Rev. 1929 (1985).

C. Transparency as Guarantee of Fairness

Predictive policing algorithms determine the fairness of the distribution of the burden of policing; they help determine who and where to target for additional surveillance.[113] In effect, they determine the quantity of law enforcement surveillance that individuals, businesses, and organizations will undergo within their community. Unguarded by the Fourth Amendment, the sweetheart of courts and scholars alike, surveillance has not received as much academic attention.[114] But, those concerned with surveillance note that surveillance is inherently discretionary[115] and costly to those the government chooses to watch.[116] Surveillance is inherently intrusive — it will encroach on subjective preferences for privacy, inhibit free expression, stigmatize, and increase the number of unwarranted police interventions.[117] The cost of this intrusion raises the question of how law enforcement determines who will bear that cost.

Predictive policing provides one answer, but predictive policing with public transparency is the better answer. When algorithms work correctly, the costs of surveillance are borne by those the government has a basis to believe are more likely engage in criminal activity or those who have the greatest need for government protection. However, as shown by the MPD, algorithms are vulnerable to clerical mistakes or flawed methodologies that result in arbitrary predictions.[118] This imposes the costs of surveillance arbitrarily across a community and removes the rational basis for those selected for greater surveillance.

---

113. PERRY ET AL., *supra* note 4, at 2.

114. Joh, *supra* note 26, at 18–19 (claiming surveillance discretion has received little scholarship).

115. *Id.* at 15.

116. *See* H.R. SUBCOMM. ON CIVIL AND CONSTITUTIONAL RIGHTS, H.R. COMM. ON THE JUDICIARY, 98TH CONG., REP. ON FBI UNDERCOVER OPERATIONS 2–3 (Comm. Print 1984) (discussing the stigma of investigations); Jeremy Gorner, *supra* note 21, (arguing investigation can lead to anxiety); Bambauer, *supra* note 25 (discussing the relevance of investigation for expression).

117. *Id. But see* Ana Viseu, Andrew Clement, & Jane Aspinall, *Situating Privacy Online*, 7 INFO., COMM., & SOC'Y 92 (arguing the classic "nothing to hide argument" that surveillance programs do not infringe on privacy unless the target is engaged in criminal activities).

118. *Cf.* E. Scott Reckard, *Data Compilers' Secret Scores Have Consumers Pegged—Fairly or Not*, L.A. TIMES (Apr. 8, 2014), www.latimes.com/business/la-fi-secret-consumer-scores-20140409,0,6240971.story [https://perma.cc/322D-NHNY] (describing clerical mistakes in the commercial context).

Additionally, algorithms that are fed biased data will perpetuate that bias.[119] Currently, certain communities are over-policed.[120] In some forms, skewed data are a result of individual officer determinations, while in other forms, department-wide determinations skew results.[121] The result is biased data reflecting disproportionate enforcement against lower-income communities and racial minorities.[122] Predictive policing that uses these data for future predictions incorporates its old biases, perpetuating them.

As discussed above, even a flawed predictive policing algorithm benefits jurisdictions through deterrence. Every member of the jurisdiction benefits from these improvements, but the flawed algorithm imposes the cost of enforcement arbitrarily among only a few members of society. In effect, a few are selected without any basis for a tax in the form of increased surveillance that benefits the entire group. Even worse, biased data can lead low-income individuals and racial minorities to pay the cost for that community benefit.[123]

One could respond that predictive policing could help to further entrench biased policing. A legitimating theory—quantitative analysis should replace policing discretion—deflects public scrutiny of law enforcement. The broken windows theory helped police justify cracking down on public nuisance crimes, and the ensuing attribution of decreases in crime to that theory further engrained it.[124] The same problem could arise where police use predictive algorithms to justify decisions if the public is unaware of its actual utility. Allowing successes to be wrongly attributed to predictive policing legitimates and builds the popularity of predictive policing models, making it harder to remove or change in the future. Biased policing in algorithms could outlive biased policing in other methods already recognized as flawed.

---

119. Joh, *supra* note 26, at 30.

120. *See generally* Eric J. Miller, *Role-Based Policing: Restraining Police Conduct "Outside the Legitimate Investigative Sphere"*, 94 CAL. L. REV. 617 (2006) (arguing some communities are over-policed).

121. *See Cost-Benefit Analysis in Criminal Justice*, POLICEONE (May 2, 2013), https://www.policeone.com/grants/articles/6218674-Cost-benefit-analysis-in-criminal-justice [https://perma.cc/63HV-5QMW].

122. Miller, *supra* note 120. *But see* Jeffrey Brantingham et al., *Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial*, 5 J. STATS. & PUB. POL. 1, 5 (2017) (failing to reject their null hypothesis that the predictive policing technology increased racial bias in Los Angeles).

123. *Id.*

124. Samaha, *supra* note 40, at 1620–32.

Transparency will allow external institutions to conduct audits and the public to pressure law enforcement to correct flawed algorithms. Combining this with my previous arguments, transparency doubles down on deterrence where algorithms are successful and fair. Where algorithms are not successful and fair, transparency provides a much-needed democratic check to ensure a fair law enforcement scheme. Despite the need for transparency with predictive policing, the current statutory scheme provides little opportunity to access the information.

IV.
RESTRICTIONS ON PUBLIC ACCESS TO PREDICTIVE POLICING INFORMATION

The process of predictive policing creates information about the algorithm or code—the dataset input into those algorithms, the incorporation of predictive policing into existing law enforcement strategies, and the predictions themselves. In this section, I address the avenues and obstacles to obtaining access to each of those forms of information.

A. Open Records Laws

Although it may appear that the existence of open records laws would ensure transparency around predictive policing, the broad exceptions to these laws frustrate that purpose.[125] Law enforcement has not traditionally shared vast amounts of internal data with the public.[126] The incorporation of technology developed by private companies, including predictive policing algorithms, has further

125. There is, of course, always the possibility that the private company elects to voluntarily release information. This degree of disclosure may not be as complete, nor is it universal across the industry, but there are companies that have done it. Letter from Michael R. Gehrman, Assistant Corp. Counsel, to J. Ader (May 18, 2018) (on file with Muckrock, https://www.muckrock.com/foi/elgin-7770/foia-elgin-police-dept-predpol-documents-51858/#file-190433 [https://perma.cc/EE9J-PNLR]) (releasing information after a court battle began); *CivicScape*, GitHub (June 5, 2018), https://github.com/CivicScape/CivicScape [https://perma.cc/K8DC-VAF4] (CivicScape released information about its technology); Josh Kaplan, *Predictive Policing and the Long Road to Transparency*, S. Side Weekly (July 12, 2017), https://southsideweekly.com/predictive-policing-long-road-transparency [https://perma.cc/7BNP-9VZB] (Chicago released information regarding predictive policing results, but not the algorithm, after seven years of refusing to provide the information.).

126. *See* Friedman, *supra* note 64.

hindered transparency.[127] When the public, whether non-government organizations or individuals, have wanted to check in on the actions of their government, they have traditionally turned to their statutory rights under open records laws.[128]

FOIA, the federal open records law, makes government information available to private citizens upon request.[129] The theoretical underpinning of the law is that access to "government information is a basic right of American citizens."[130] Transparency provides the public the ability to scrutinize government actions and, thus, hold their government accountable.[131] Given the rights-based notion of FOIA, records are made available regardless of purpose or motivation such that "even a person with only 'idle curiosity' may request disclosure of information."[132]

While FOIA favors open access to government activity, it still balances the public's right against the interest of the government in keeping some information secret.[133] The act has a number exceptions for information pertaining to national defense, foreign policy, law enforcement, commercial trade secrets, and other categories of information that could cause harm to the government or other parties if shared with the general public.[134] A substantial number of statutory guidelines and judicial decisions delineate the boundaries of each of these categories.[135]

---

127. *See* Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979) (recognizing a private sector interest in secrecy in the decision to not disclose information).

128. Several legislatures have expressly recognized the purpose of open records laws is to create transparency in government. 37A AM. JUR. 2D, Freedom of Information Acts § 2.; Cal. Gov. Code § 6250; 5 ILL. COMP. STAT. 140/1 to 140/2 (2010).

129. *See, e.g.*, Renegotiation Bd. v. Bannercraft Clothing Co., 415 U.S. 1, 18 (1974) (recognizing the process by which FOIA achieves government transparency).

130. Monique C.M. Leahy, *Proof Supporting Disclosure under State Freedom of Information Acts*, 132 AM. JUR. PROOF OF FACTS 3d 1 (2013) (arguing access to government information is a basic right).

131. *See* 37A AM. JUR. 2D, Freedom of Information Acts § 1; ACLU v. U.S. Dept. of Justice, 750 F.3d 927 (D.C. Cir. 2014).

132. San Lorenzo Valley Community Advocates for Responsible Educ. v. San Lorenzo Valley Unified Sch. Dist., 139 Cal. App. 4th 1256 (6th Dist. 2006).; 37A AM. JUR. 2D, Freedom of Information Acts § 408. (stating a requestor need not state a reason).

133. McKinley v. F.D.I.C., 744 F. Supp. 2d 128 (D.D.C. 2010), judgment aff'd, 647 F.3d 331 (D.C. Cir. 2011).

134. 37A AM. JUR. 2D, Freedom of Information Acts § 1.

135. *See* 5 U.S.C.A. § 552(b)(1) (West 2006) (providing the categories of FOIA exemption).

The fact that predictive policing algorithms are privately-developed does not alone render FOIA inapplicable. Even government files originally created by private citizens often become subject to FOIA once in the possession of the government.[136] For example, in *TJS of New York, Inc. v. New York States Dept. of Taxation and Finance*, software sold to the government by a private contractor became a record of an agency. Upon a FOIA request, the court required the software shared with another private citizen over the objections of both the government agency and the government contractor.[137]

Although FOIA does not apply to data shared only with state and local governments,[138] each of the fifty states and many cities have their own open records law. State open records laws are modeled on the federal law[139] and share the same transparency goals as FOIA.[140] Given these similarities in language and purpose, courts draw on federal jurisprudence to interpret their state analogues.[141] Case law on FOIA is thus especially persuasive precedent in state decisions, and courts often draw comparisons across jurisdictions. Therefore, I incorporate both federal and state decisions to illuminate the likely outcome of open records requests for predictive policing information. Despite the need for transparency, I expect that business information and law enforcement exceptions to FOIA disclosure will impair the potential for openness with predictive policing.

---

136. *See* U.S. Dept. of Justice v. Tax Analysts, 492 U.S. 136, 144 (1989) (articulating a two-part for determining what constitutes an agency record).

137. TJS of N.Y., Inc. v. N.Y. State Dep't of Taxation & Fin., 89 A.D.3d 239, 241 (2011) (ruling software acquired by the government subject to New York open records law).

138. Elizabeth O. Tomlinson, *Litigation Under Freedom of Information Act*, 110 Am. Jur. Trials 367 (2017) ("FOIA is a federal act and as such, it does not apply to state or local governments.").

139. *See, e.g.*, Ala. Code § 36-12-40 (1975). *But see* David L. Ganz, *Open Public Records Act Litigation*, 128 Am. Juris. Trials 495 (2017) (FOIA "imposes no affirmative obligation to unilaterally disclose information," whereas state laws "permit or require disclosure by public authorities to the population as a whole.").

140. *See, e.g.*, Thomas v. Hall, 2012 Ark. 66, 399 S.W.3d 387 (2012); ACLU Found. of S. Cal. v. Superior Court of L.A. Cty., 186 Cal. Rptr. 3d 746 (Cal. Ct. App. 2d Dist. 2015); Cent. Fla. Reg'l Transp. Auth. v. Post-Newsweek Stations, Orlando, Inc., 157 So.3d 401 (Fla. 5th DCA 2015); Office of the Governor v. Davis, 122 A.3d 1185, 1191 (Pa. Commw. Ct. 2015); Predisik v. Spokane Sch. Dist. No. 81, 346 P.3d 737, 739 (Wash. 2015).

141. Leahy, *supra* note 130 ("Because the state acts usually have been modeled on the Federal FOIA, courts draw on the federal counterpart for judicial construction and legislative history.").

B. The Business Information Exception

1. The Structure and Applications of the Exception

The business information exception to FOIA disclosure prevents required disclosures of certain business-related information.[142] Commercial law protects company profits by allowing companies to keep trade secrets, a doctrine which also applies to trade secrets shared with the government.[143] For example, the trade secrecy doctrine protects the design of privately developed voting machines.[144]

A number of non-physical assets fall under the category of trade secrets. The law protects business-related information if (i) there is economic value from the information not being generally known to other persons who could obtain economic value from its disclosure and (ii) there have been reasonable efforts to maintain its secrecy.[145] The law protects company formulas, compilations, programs, devices, methods, and processes.[146]

Applying the law to the voting machine example, there exist company designs for the physical machine and information about how to keep votes safe from cyber-attacks. There also exists a system for tabulating votes entered on the machines. A voting machine company profits from protecting that information from competitors who might, for example, use it to undercut their government contracts or develop improved machinery. To avoid these situations, the company may use passwords on its computers, release info only on a "need to know" basis, require employees or purchasers to sign confidentiality agreements, or issue verbal instructions to those they work with not to reveal the information.[147] As long as the voting machine company makes reasonable efforts to protect that

142. 5 U.S.C.A. § 552(b)(4) (West 2016).

143. RESTATEMENT (FIRST) OF TORTS § 757 cmt. B (AM. LAW INST. 1939) (describing trade secrets doctrine generally); *see* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 147 (2007) (describing the protection of trade secrets of the government under the same commercial doctrine applied to trade secrets held by private actors). The Freedom Of Information Act exception also protects matters that are "commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C.A. § 552(b)(4) (West 2016).

144. *About*, DIEBOLD ELECTION SYSTEMS, https://www.dieboldnixdorf.com/en-us/about-us (last visited Sept. 8, 2018).

145. Uniform Trade Secrets Act § 1(4).

146. *Id.*

147. See Liberty Am. Ins. Grp., Inc. v. Westpoint Underwriters, L.L.C., 199 F. Supp. 2d 1271 (M.D. Fla. 2001); RKI, Inc. v. Grimes, 177 F. Supp. 2d 859 (N.D. Ill. 2001); Equifax Servs., Inc. v. Examination Mgmt. Servs., Inc., 453 S.E.2d 488 (Ga.

information, the trade secrets doctrine protects the company's information from falling into the hands of potential competitors.[148]

Given its importance to private industry,[149] the trade secrets doctrine has been incorporated into Exemption Four of FOIA, which protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."[150] The exception technically covers two categories of information. The former provides protections under a more technical definition of trade secrets, while the latter builds upon the underlying policy of trade secrets doctrine to cover privileged and confidential commercial information generally. The "commercial or financial information" category is much broader and applies to "anything pertaining or relating to or dealing with commerce."[151]

State law reflects FOIA and the federal courts' interpretation of the exemption, including the protection of source codes as trade secrets.[152] For example, Illinois includes trade secrets and commercial information in the same two distinct categories.[153] On the whole, both federal and state open records laws allow the government, or a private contractor, to claim that an information request should be denied on IP grounds.

Ct. App. 1994); Fred's Stores of Miss., Inc. v. M & H Drugs, Inc., 725 So. 2d 902 (Miss. 1998).

148. *See, e.g.*, Cisco Sys. Inc. v. Lynn, No. 05-CV-03043 (N.D. Cal. Jul. 27, 2005).

149. *See* Wesley M. Cohen, Richard R. Nelson, & John P. Walsh, *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)* 13 (Nat'l Bureau of Econ. Research, Working Paper No. 7552, 2000), http://www.nber.org/papers/w7552.pdf [https://perma.cc/6HLZ-2LJP] (finding among 1,478 manufacturing firms, secrecy ranked first or second in importance for product innovations).

150. 5 U.S.C. § 552(b)(4) (West 2016); *see also* Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871, 879 (D.C. Cir. 1992) (holding voluntary submission to the government did not waive trade secrecy rights and trade secrets must only satisfy any one prong of the FOIA exception). Was this holding that any one of the prongs is enough or was it one specific prong?

151. American Airlines, Inc. v. National Mediation Bd., 588 F.2d 863, 870 (S.D.N.Y. 2003).

152. *See generally* Leahy, *supra* note 130 (describing structure of state open records laws). Source codes are simply the building blocks of any computer program. Maybe add a little bit of background on source codes or an example of when a source code could be treated as a trade secret.

153. *See* 5 ILL. COMP. STAT. 140/7(1)(g)(ii) (2018). Illinois strays from the structure of the federal law by leaving agencies discretion over whether to disclose some trade secrets and confidential information, whereas FOIA mandates secrecy. *Id.*

Business information exceptions extend to types of information similar to predictive policing algorithms. These exceptions have protected source codes,[154] as well as computer software and proprietary technology.[155] Also, they have protected the structuring and informational basis for these technologies, including predictive technologies. Proprietary technology provided Illinois law enforcement with the rationale to deny disclosure of the ten variables used in a predictive policing algorithm.[156] There exists a substantial foundation in both federal and state court decisions for denying open records laws requests for information related to the IP of private government contractors. This foundation lays the groundwork for excluding predictive policing information from the public eye as well, stymying critical public oversight efforts.

2. The Rationale for Extending the Business Information Exception to Predictive Policing

Courts could extend the business information exception to predictive policing, but such extension would be detrimental to the public's ability to hold law enforcement accountable. In the next two sections, I explain how courts could arrive at the conclusion that predictive policing information should be kept secret before showing why that conclusion would be a mistake. Preventing the disclosure of information serves the interests of companies engaged in or likely to engage in contracts with the government.[157] Because private companies currently sell predictive policing technology to the government, the same interests apply. Given the government's emphasis on protections for small businesses, those commercial protections are arguably even more important for predictive policing companies, which are typically small.[158] Because the disclosure of information may place American companies at a competitive dis-

154. *See, e.g.*, GlobeRanger Corp. v. Software AG United States of Am., 836 F.3d 477 (5th Cir. 2016).

155. See 48 C.F.R. § 52.227-14(a) (defining for civilian acquisitions "data" as including computer software).

156. Davey, *supra* note 22.

157. *See* Nathan T. Nieman, Note, *Reforming the Illinois Freedom of Information Act: An Opportunity to Repair the Leaky Boat*, 58 DEPAUL L. REV. 529, 556 (2009) (arguing the Illinois FOIA ought to expressly notify parties whether their trade secrets will be disclosed to increase its protections for economic growth).

158. The Small Business Act in 1953 recognized the importance of small businesses to the United States economy. 15 U.S.C.A. § 631 (West 2010). Many predictive policing companies, like PredPol, are small businesses. PredPol, Inc., Notice of Exempt Offering of Securities (Form D) (June 16, 2014) (reporting a revenue between $1 million and $5 million). *But see* IBM Reports 2016 Fourth Quarter and Full-Year Results (Jan. 19, 2017), https://www.ibm.com/investor/att/pdf/IBM-

advantage,[159] there is a purely economic justification for the trade secrets exception. Predictive policing companies are a part of that economy, so the exception applies.

Protecting the IP of predictive policing companies helps to ensure law enforcement can continue to obtain the technology by incentivizing market participation. Recall that predictive policing can provide substantial benefits to police departments, but it can only provide those benefits if private companies continue to develop and sell the technologies. Removing the ability of predictive policing companies to turn a profit could result in smaller companies losing the support of venture capital investors or larger companies substituting more profitable products for their current predictive policing projects.[160] Limitations on remedies further disincentivize investment.[161] More likely than exiting the market, private companies will raise their prices to account for the increased risk of government contracting.[162] This will result in larger outlays for the technology from law enforcement, greater opportunity costs, and fewer cities being able to afford the technology.

There is a final ramification of decreased expected profits that relates specifically to the market fragmentation of predictive policing.[163] The available capital of small companies is more likely to limit the development of predictive algorithms than for large companies.[164] Small companies can only design so sophisticated a model because they can only invest so much before making a sale. Decreasing IP protections for predictive policing companies en-

4Q16-Earnings-Press-Release.pdf [https://perma.cc/ZL9U-WWZH] (reporting annual revenue in 2016 of $32.8 billion).

159. *See* Cohen, Nelson, & Walsh, *supra* note 149 (finding IP important for company innovation).

160. Nader Mousavi & Matthew J. Kleiman, *When the Public Does Not Have a Right to Know: How the California Public Records Act is Deterring Bioscience Research and Development*, 2005 DUKE L. & TECH. REV. 23, ¶ 29.

161. One such limitation on recovery is the inability to receive an injunction against the government for data disclosure. *See* 48 C.F.R. § 52.233-1. Another limitation is the doctrine of "waiver," which requires the government to reveal information it would otherwise keep secret because it previously disclosed the information. *See* Watkins v. U.S. Bureau of Customs & Border Prot., 643 F.3d 1189, 1198 (9th Cir. 2011).

162. *See* Mousavi & Kleiman, *supra* note 160 (suggesting companies may raise prices to account for unpredictable IP rights).

163. Cherry & Rogers, *supra* note 107.

164. The economic principles I discuss in this paragraph do not extend beyond the fundamentals and can be found in any introductory economics text. *See e.g.*, N. GREGORY MANKIW, PRINCIPLES OF ECONOMICS 272–73 (2012) (discussing how economies of scale for larger companies can increase efficiencies and free up capital).

hances the' risk that they will start producing even less sophisticated models. The reduced protections incentivize smaller investments with faster returns. Less sophisticated models may not be inherently bad, but earlier I noted that many of the weaknesses of predictive policing relate to potential flaws in the models. A favorable economic environment, together with a demand for fairer models, could help start to resolve those concerns. Moreover, better models could promise greater effectiveness and efficiency in law enforcement, doubling down on the benefits of predictive policing.

In sum, limited IP protections weaken the market for the technology and potentially the quality of the technology itself. Because investments in predictive policing rely almost entirely on intellectual assets rather than physical assets, IP rights assume a determinative role in business decisions. With government contracting in predictive policing technology, the industry turns on the guarantee of these rights.

Even if there is a solid justification for strong IP concerns here, why do companies require secrecy to protect their IP? The trade secrets doctrine is not the only means of protection. Private companies could also rely on copyright or patent law.[165] However, each of these measures is unlikely to satisfy many predictive policing investors, especially if the investment is a more sophisticated predictive algorithm.[166]

IP rights present for private developers two additional hurdles. First, the rights attach automatically upon creation of the work, but protect "only the physical embodiment" not the "concepts or ideas underlying the work."[167] Much of what differentiates one predictive model from another are inventive variables and combinations of data. Even if a company does not copy another's predictive model verbatim, copying the underlying ideas behind the model could undercut a company's competitive advantage. Trade secrets, unlike copyrighted materials, do not require one to make "an exact or nearly exact copy of an algorithm or complication of information to

165. Nancy O. Dix et al., *Fear and Loathing of Federal Contracting: Are Commercial Companies Really Afraid to Do Business with the Federal Government? Should They Be?*, 33 PUB. CONT. L.J. 5, 11 (2003) ("An example of a product-specific issue is software, which in certain cases may be entitled to both patent and copyright protections.").

166. With both protections, private actors can only pursue damages in a suit against the government, not any injunctive relief. *See* Levine, *supra* note 143, at 178.

167. 17 U.S.C.A. § 102 (1976).

be liable . . . ."[168] Second, there are limits on copyright rights in government contracting. Government permission is often required both to copyright works first produced under a government contract and to include copyrighted work in deliverables to the government.[169]

Like copyrights, patents also fail to protect the underlying ideas of the predictive algorithms. Patents have been filed for predictive policing and arguably provide more appropriate protections than copyrighting.[170] Yet, patentees of predictive technology may still fear that their now public algorithms will be ripped off by competitors given the importance of discrete decisions and ideas within the models.[171] Developers of predictive technology also face a difficult choice ex ante. If they obtain a public patent for their technology, they must indefinitely rely upon the patent for their protection because they are no longer able to argue that the technology is a trade secret.[172] Trade secrets may be converted to patented material. Uncertainty of their future situation could drive predictive policing companies into the arms of trade secrecy law instead of patent law because doing so lends them the flexibility to change their mind and obtain a patent at a later date.

I am not arguing that these financial determinations are an adequate justification for keeping predictive policing secret. I am simply showing that the policy-focused FOIA determinations of courts could fit the algorithms under this exception of an open records law. Given the current situation of the predictive policing industry, private actors have the incentive to push for greater IP protections, and courts have a platform to recognize those interests. The current law provides both a committed advocate for secrecy and a legal ground from which to argue for that secrecy.

C. The Law Enforcement Exception

1. The Exception in General

Courts could also reduce transparency by fitting algorithms under law enforcement exceptions to open records laws. These exceptions protect "records compiled for law enforcement pur-

168. Michelle L. Evans, *Establishing Liability for Misappropriation of Trade Secrets*, 91 Am. Juris. Proof of Facts 3d 95 (2017) (referencing Restatement (First) of Torts § 757 (Am. Law Inst. 1939)).

169. FAR 52.227-14

170. *See, e.g.*, U.S. Patent No. 8,949,164 (issued Feb. 3, 2015). .

171. Dix et al., *supra* note 165, at 13–14.

172. *Id.*

poses."[173] The exceptions define law enforcement broadly to include everything from surveillance tactics to immigration enforcement techniques and strategies to uncover tax fraud.[174] The underlying theme that connects these categories is an intent to enforce a law or regulation, and courts have denied the exception for any other purpose, pretextual rationale, or improper use.[175] The law remains grounded in the advancement of law enforcement, and so most circuits apply less exacting standards when considering exemptions for police departments than when considering the same exemptions for other agencies.[176]

A number of judicial and statutory limitations help to define the scope of law enforcement exceptions and capture their purpose. Statutes contain specific limitations on what constitutes a law enforcement purpose, and courts balance law enforcement justifications against public interests in disclosure.[177] Although the numbering and language of statutes vary, most hew closely to the limits provided in FOIA.[178] Sections 7(C) and 7(E) of the federal statute allow exemption under the law enforcement rule when the production of ". . . law enforcement records or information . . .

(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, . . .

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law . . ."[179]

7C protects personal information that law enforcement gathers and uses for legitimate purposes. 7E addresses information about the law enforcement strategies themselves. Although state codes may change the formatting, they generally reflect the same protec-

173. 5 U.S.C. § 552(b)(7)(A); Jordan v. U.S. Dep't of Justice, 668 F.3d 1188 (10th Cir. 2011).

174. U.S. DEP'T. OF JUST. MANUAL U.S. ATT'YS MANUAL § 3-17.100 (describing potential application of law enforcement exceptions).

175. *Id.*

176. *See, e.g.*, Puerto Rico v. U.S. Dep't. of Justice, 823 F.2d 574, 583–84 (D.C. Cir. 1987) (applying a rational nexus test).

177. This occurs especially in state court decisions. *See, e.g.*, Chicago All. for Neighborhood Safety v. City of Chicago, 808 N.E.2d 56, 73 (Ill. App. Ct. 2004); ACLU of Oregon, Inc. v. City of Eugene, 380 P.3d 281, 284 (Or. 2016).

178. *See* Tomlinson, *supra* note 138, at 367.

179. 5 U.S.C. A. § 552(b)(7) (2000). These are only two sections of several other possible law enforcement sections. I only mention these two because they are the exceptions most directly applicable to predictive policing.

tive goals. The limits to the FOIA law enforcement exception demonstrate the statute's commitment to ensuring an enforcement purpose. Courts further respect that purpose by limiting the exception temporally — the exception only applies so long as there is an active law enforcement proceeding or investigation that demands secrecy.[180]

2. The Exception's Applicability to Predictive Policing

Both 7C and 7E could apply to predictive policing. Exception 7C may apply to predictive policing because the algorithms generate data specific to individuals. Protection of personal information includes not just big data information like addresses, credit scores, incomes, and such, but also an individual's status as a target for additional surveillance. In *Union Leader Corp. v. U.S. Department of Homeland Security*, the Court prevented disclosure of a list of names because doing so would reveal the characteristics that put an individual on the list and the surveillance consequences for those individuals.[181] The court determined that the traits that merit police suspicion also merited privacy. To the extent that predictive policing can generate lists of individuals likely to be involved with crime, *Union Leader Corp.* would justify secrecy with the outputs of individual-based algorithms. Even if the determinative variables are harder to isolate with predictive policing than normal strategies, the stigmatizing impact from mere association with any law enforcement investigation constitutes a ground for applying Exception 7C.[182]

Although less apparent than individual-based predictions, an argument also exists for concealing information related to location-based predictive policing. Revealing location-based predictions may in effect disclose individuals or businesses residing within that location. The emphasis on stigmatization from *Union Leader Corp.* furthers this argument. For example, a business located within an area that an algorithm predicts will see more violent crime will understandably receive less business after that prediction is made public through a FOIA request. The argument that location-based predic-

180. Citizens for Responsibility & Ethics in Washington v. U.S. Dep't of Justice, 746 F.3d 1082, 1097 (D.C. Cir. 2014) ("Exception 7(A) is temporal in nature.").

181. *See* Union Leader Corp. v. U.S. Dep't of Homeland Sec., 749 F.3d 45, 51–53 (1st Cir. 2014).

182. Shapiro v. U.S. Dep't of Justice, 34 F. Supp. 3d. 89, 95–97 (D.D.C. 2014) ("Exemption 7(C) recognizes that the stigma of being associated with any law enforcement investigation affords broad privacy rights to those who are connected in any way . . ."). Also note, individual-based arguments could also apply to targeted organizations, businesses, or advocacy groups.

tions can still embarrass, stigmatize, and expose to public scrutiny members of the community has particular application to precise predictive technologies that can make predictions as narrow as a 400 x 400 foot square.[183] Personal information concerns help to protect the inputs and outputs of algorithms from the disclosure under open records laws.

Exception 7E could serve to protect the algorithms themselves. Strategy exceptions can justify not disclosing information that may reach investigatory targets, but those justifications evaporate once the prediction-based surveillance ends and a new prediction takes its place. Because the same algorithm is used in current and future predictions, transparency before the surveillance or investigation ends provides criminals the means to figure out what the models will predict and circumvent law enforcement. Therefore, the predictions themselves have a limited lifespan of protection under 7E, while the algorithms and computational methods have an indefinite lifespan under 7E.[184]

The burden of proof placed on the government is easily met, which simplifies the task of keeping algorithms secret. The government need not prove disclosure *will* allow circumvention of the law, only that it *risks* circumvention.[185] In addition, the exception's broad language encompasses many law enforcement records. Guidelines include any "means by which agencies allocate resources for law enforcement investigations." Techniques and procedures include "the means by which agencies conduct investigations."[186] Between these two categories, protections extend as far as law enforcement manuals, policy guidance documents, settlement guidelines, monographs, and emergency plans.[187]

Precedent benefits agencies attempting to fit predictive policing algorithms under exceptions to protect law enforcement goals. The algorithms help determine the distribution of officers and constitute a procedure through which agencies conduct investigations. Moreover, precedent suggests investigations within the meaning of the FOIA exception need not be suspicion-based, which means pre-

183. PERRY ET AL., *supra* note 4, at 65 (explaining how precise algorithms predictions can be).

184. 7E protects techniques and procedures for law enforcement, which would include predictive policing techniques and the strategies implementing it. 7E also protects guidelines where transparency would risk circumvention of the law. Guidelines on how to determine resource allocation under predictive policing would fit under this second clause.

185. 5 U.S.C.A. § 552(b) (7)(E) (West 2016).

186. Tomlinson, *supra* note 138.

187. *Id.*

dictive algorithms are protected even though they are generally used at the surveillance stage of law enforcement action.[188] In *American Civil Liberties Union of New Jersey v. FBI*, an FBI racial mapping initiative was exempted because revealing the distribution of future surveillance efforts would interfere with later enforcement proceedings and reveal the targets of those efforts. Similarly, in *Showing Animals Respect and Kindness v. U.S. Department of the Interior*, documents on surveillance equipment used to locate and time potential poachers was exempted because it risked circumvention. These decisions lend credence to the idea that efforts to determine where to focus future surveillance can receive protection through exemption. The broad scope of this provision provides ample room for placing new law enforcement devices under its wing and preventing public oversight.

Additional grounding for the inclusion of predictive policing under Exception 7E comes from prior decisions including similar technologies. Previous cases have recognized the ability to exempt information on drones and drone use in surveillance measures from open records actions.[189] Proponents of secrecy can argue that revealing information about advanced technologies defeats law enforcement's ability to stay one step ahead of criminals and criminal organizations.[190] Such arguments have successfully exempted information systems and computer systems used for tracking movements of criminal activity, as well.[191] Unfortunately for transparency advocates, a sophisticated predictive algorithm would also likely fall within these exemptions.

---

188. ACLU of New Jersey v. FBI, 733 F.3d 526 (3d Cir. 2013); Asian Am. Legal Def. & Educ. Fund v. New York City Police Dep't, 964 N.Y.S.2d 888 (2013).

189. Electr. Privacy Info. Ctr. v. Customs & Border Prot., 160 F. Supp. 3d 354, 261 (D.D.C. 2016) (granting in part and denying in part a FOIA request because the drone information could fit within Exemption 7(E) but the agency failed to provide sufficient justification for why the Exemption should apply in that particular case); Citizens for Responsibility & Ethics in Washington v. U.S. Dep't of Justice, 746 F.3d 1082, 1092 (D.C. Cir. 2014) (finding for the plaintiff on similar grounds).

190. Aff. of FBI Supervisory Special Agent Bradley S. Morrison, Chief, Tracking Technology Unit, Operation Technology Division in Quantico, Virginia, at 2, Apr. 11, 2014, attach. to City's Verified Answer, Hodai v. City of Tucson, No. C20141225 (Ariz. Super. Ct. Apr. 14, 2014).

191. Skinner v. U.S. Dep't. of Justice, 893 F. Supp. 2d 109, 112–13 (D.D.C. 2012) (properly withholding computer access codes for information systems); Bishop v. U.S. Dep't. of Homeland Sec., 45 F. Supp. 3d 380, 389 (S.D.N.Y. 2014) (protection system for tracking individuals).

3. Reasonably Segregable Exception

Even where courts rule some information about predictive policing may be disclosed without risking circumvention of the law or invasions of personal privacy, the "reasonably segregable" requirement protects the rest of the information. Written into FOIA and state open records laws, the reasonably segregable requirement requires agencies to disclose portions of the record that do not fall within an exception when they can be separated from the rest of that record.[192] This means the public can gain access to some information that might otherwise be exempted, but also that courts avoid tough decisions for full disclosure by allowing partial disclosures. With as complicated a tool as predictive policing, partial disclosures will likely fail to provide sufficient insight to really understand how the models are operating within law enforcement.[193] Likewise, courts can require agencies to disclose techniques in only general terms without any specifics,[194] again making it difficult to complete a rigorous analysis of the predictive technology and its use. Partial disclosures have made external audits and accountability difficult in the context of other sophisticated law enforcement tools and would also allow only a shallow analysis of predictive policing.[195]

Over the last several decades, police departments have developed a culture of silence, preferring to keep information secret rather than disclose it to the public.[196] In the context of FOIA, even law enforcement agencies that favor transparency with predictive policing have incentives to deny open records requests and fight court orders. First, "voluntary disclosure in one situation can preclude later claims that records are exempt from release to someone

192. Tomlinson, *supra* note 138.

193. Chris J. Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 598 (arguing multiple documents are necessary to provide context to understand FOIA responses); Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy*, 28 HARV. J. L. & TECH. 1, 39 (2014) (arguing that heavily redacted documents defeat the utility of many FOIA requests).

194. Tomlinson, *supra* note 138.

195. *See supra* pp. 23–25.

196. *See, e.g.*, Jerome H. Skolnick, *Corruption and the Blue Code of Silence*, 3 POLICE PRAC. & RES. 7 (2002); Jeremy R. Lacks, Note, *The Lone American Dictatorship: How Court Doctrine and Police Culture Limit Judicial Oversight of the Police Use of Deadly Force,* 64 N.Y.U. ANN. SURV. AM. L. 391 (2008); Gabriel J. Chin & Scott C. Wells, *The "Blue Wall of Silence" as Evidence of Bias and Motive to Lie: A New Approach to Police Perjury,* 59 U. PITT. L. REV. 233 (1998).

else."[197] A law enforcement agency may feel completely comfortable revealing predictive policing information to the ACLU with the understanding that an external review may improve legitimacy and effectiveness. However, the agency will not have the same positive effect for suspected members of criminal organizations, but still find itself bound to disclosure because of its previous cooperation with the ACLU's request. Second, FOIA decisions create precedent for future disclosure or non-disclosure. With courts comparing technologies in FOIA decisions, police departments that put up little fight to the disclosure of predictive policing force themselves into a much greater conflict over the disclosure of the next big thing in policing, whatever it may be. Departments fear negative precedent for requests for predictive technology requests, as well as requests for whatever the next big thing in policing becomes.

Concerns over evasion of the law lends law enforcement a strong argument for fitting predictive policing information under the current exception. Predictive technologies are designed to help police departments determine where to send officers. If the public knows how those predictions are made, then criminal organizations can avoid those locations. Ensuring law enforcement can continue to function effectively is part of the rationale for balancing tests and the litany of complicated exceptions. Pure transparency is unlikely in this context, as experience with previous technologies demonstrates below.

D. The Unlikelihood of Accessing Predictive Policing Information

The public's difficulty getting information with Stingrays exemplifies the quintessential problems the public will face getting information about predictive policing.[198] Stingray technology allows police to track individuals by tracking the movement of their cellphones. The cellphones ping off of cell towers installed with the stingray technology. Illinois law enforcement used Stingrays for years without the public being fully aware of that use. The Stingray story did eventually break, and attorneys applied for information under the state open records law. They waited for a response from law enforcement for months. Ultimately law enforcement delivered the information, but the documents were so heavily redacted much of the attorneys' inquiries could not be answered. Meanwhile, police had begun to use the Stingrays to track protestors of the po-

197. Lieber v. Board of Trustees of S. Ill. Univ., 680 N.E.2d 374 (Ill. 1997) (citing Cooper v. U.S. Dep't of the Navy, 594 F.2d 484, 485–86 (5th Cir. 1979)).

198. Pell & Soghoian, *supra* note 193, at 34–39. My information about the stingray technology and this story come from the article by Pell & Soghoian.

lice.[199] Transparency was slow and half-hearted, and because of that fact, accountability was negligible.

Receiving information about predictive policing will likely be more difficult. Unlike Stingrays, where the concern is the implementation of the technology (for example, tracking police protestors), predictive policing raises concerns about the design of the technology. Predictive policing also presents a much more complex question. Information exists about inputs, algorithms, outputs, and implementation. Each of those steps involves a point where the public could demand public accountability and oversight. The number of steps also presents more opportunities for information to fall into an exception to open records laws. The complexity of predictive policing also makes it more difficult to know what to request from law enforcement. Asking: "Are you using Stingrays and for what purpose?" opens and closes the discussion. That same question is just a starting point with predictive policing, for the strategy also includes questions about algorithm design, inputs, and beyond.

In sum, the current legal framework provides little opportunity for substantial transparency with predictive policing.[200] Executive agencies, the judiciary, and the legislature have each proven themselves mediocre conduits of law enforcement information to the public. More importantly, relying on any government institution perpetuates the problems inherent in government-citizen informational gaps. Organizations, like civilian review boards, may better convey that information to the public and alleviate legitimacy concerns about creating an inner-circle of politicians and bureaucrats in the know. However, civilian review boards have yet to catch on, so the public's primary opportunity for predictive policing information remains open records laws. Without transparency, there is little

199. *Id.* at 34–39.

200. There has been *very* little litigation on this subject matter. What litigation that has occurred has produced mixed results. In Los Angeles, a non-profit's request for predictive policing information was denied. Brenda Gazzar, *Activists File Lawsuit over LAPD's Predictive Policing Program*, GOV'T TECH. (Feb. 14, 2018), http://www.govtech.com/public-safety/Activists-File-Lawsuit-Over-LAPDs-Predictive-Policing-Program.html. Others, such as the Brennan Center in New York, have made more success. Rachel Levinson-Waldman & Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, BRENNAN CTR. FOR JUSTICE (Jan. 26, 2018), https://www.brennancenter.org/blog/court-rejects-nypd-attempts-shield-predictive-policing-disclosure [https://perma.cc/4RAB-5JC9] (gaining access through the courts to email correspondence, some historical output data, notes from the developer, a summary of results of trials on the products, and policies regarding the technology, but not receiving the algorithm itself).

opportunity for oversight over this new, rapidly evolving technology.

CONCLUSION

Transparency has long been extoled as a requisite and virtue of democracy. Predictive policing's unique characteristics emphasize this need for transparency. Despite this heightened need, the momentum behind open records laws may sweep predictive policing under confidential business information and law enforcement exceptions. In this gap between normative ideals and positive expectations, exists an opportunity for practitioners to distinguish the unique need for transparency with predictive policing from other law enforcement methods. Establishing that precedent now lays a foundation for similar arguments in the continuously developing field of predictive analytics. While practitioners work to distinguish predictive policing to help craft precedent favoring transparency, lawmakers should turn their focus to how the language of open records laws fails to differentiate among technologies and consider creating exceptions for novel police technologies like predictive policing.

While total transparency may not be feasible with predictive policing, drawing the line with too blunt a tool threatens to leave the public in the dark about the realities of this new tactic. Given the growing coordination between the public and private sectors in areas like law enforcement, the increasing reliance on sophisticated technology, and disparities in information about those technologies, the challenge to transparency has grown more complex and the need for transparency more acute. Predictive policing demonstrates why attorneys cannot concede that difficult battle.