“It makes almost no difference which algorithm you use”: On the modularity of predictive policing

Nick Lally
Assistant Professor
Department of Geography
University of Kentucky
nicklally@uky.edu
“It makes almost no difference which algorithm you use”: On the modularity of predictive policing

Abstract: Place-based predictive policing software is built on a simple assumption: crime exhibits predictable patterns, which means future crime risk can be forecasted using computational methods trained on historic crime data. Software developers argue that their software allows police departments to more accurately and precisely deploy officers to problem areas, which shift in both time and space, thus making more efficient use of finite resources. While critics have raised concerns over the widespread use of biased data in these systems, less is known about how software is actually put to use when integrated into infrastructures of governance. Drawing on interviews with software developers and an analysis of technical, promotional, and academic materials, I show how internal and external pressures separate predictive policing from the concrete practices it attempts to transform. I argue that predictive policing is a modular technology, plugged into the black box of policing. This modularity separates software developers from the practices that they attempt to transform, while enabling them to deflect criticism away from the programs they build. Modularity also means that software can be reconfigured and connected to other systems, which threatens to undermine the set of best practices that guide its development.

Abstract: police, algorithms, predictive policing, modularity, digital geographies
Introduction

In the offices of private software companies and in university laboratories—far removed from the streets where police patrol—software developers produce methods to analyze and interpret crime data. The statistical and machine learning methods developed are integrated into mapping software with the intention of informing the future spatial distribution of police patrols. Place-based predictive policing, which is the subject of this article, is built on a simple premise: crime exhibits predictable patterns, which means future crime risk can be forecast using computational methods trained on historic crime data. Vendors of predictive policing promise their software will enable police departments to more accurately and precisely deploy officers to problem areas, which shift in both time and space, thus making more efficient use of finite resources. Software vendors argue that officer presence in those areas will deter crimes from ever happening—a narrative that elides the material violence of everyday practices of policing as crime simply vanishes into thin air.

The narrative of policing as a crime deterrent runs up against growing public concern over the violent and racist practices of policing. Cell phone videos of police violence have been widely reported and shared in recent years, sparking massive protests and the growth of movements like Black Lives Matter. While over-policed communities have long decried police presence and violence, the recent proliferation of video evidence—much of it enabled by the ubiquity of smartphones and spread through social media—has led to growing public questioning of policing practices, especially amongst people of color, young people, and progressives (Norman, 2017; Morin, Parker, Stepler, & Mercer, 2017). The increasing public visibility of racism in policing, as many have observed, does not mean racist policing is a new phenomenon. As an institution, policing in the United States can trace its roots back to slave patrols. W.E.B. Du Bois (1998) argued that slavery required a police force—a force that relied upon, exploited, and fed the racism of poor southern whites who it enrolled. In the policing technologies of slavery, including fugitive slave ads and lantern laws, Simone Browne (2015) locates precursors to contemporary mass surveillance technologies. While contemporary institutions of policing might publicly denounce the racism of their roots, they still work towards producing, enforcing, and amplifying racialized difference. Rashad Shabazz (2015), for example, argues that policing acts in concert with urban planning and architecture to produce “spatialized blackness” as the city comes to mirror the logic of the prison for its Black inhabitants. These logics, as they leak out of formal structures of incarceration, result in the “intense regulation of low-income communities of color as prisonlike spaces themselves” (Vitale & Brian Jordan, 2016, p. 158) Simultaneously, policing places a central role in maintaining massive prison populations in the United States by “removing people from disordered, deindustrialized milieus and depositing them elsewhere” (Gilmore, 2007, p. 14). Disproportionately represented in prison populations, people of color become enrolled within the justice system through their contacts with the police, feeding the prison industrial complex’s expanding ability to secure capitalist profit (Davis, 2003).

Policing in the United States not only reinforces racialized inequities, it reflects, amplifies, and targets other forms of difference. Transgender people, for example, report widespread mistreatment by police during interactions (James et al., 2016). So too are intersecting categories of gender, race, and disability often met with the violence of policing (Ritchie, 2017). Although data is spotty, people living with mental illness are disproportionately the victims of police violence as police often become de facto first responders to many mental health crises (Lane-McKinley, Tsungmey, & Roberts, 2018). Hot spots targeted for police
interventions have been correlated with higher rates of mental and physical illness (Weisburd & White, 2019). Police violence in its uneven distribution often turns deadly. Media outlets estimate over 1000 people are shot and killed by police every year in the U.S., although there is no official, centralized data kept on those statistics.¹

Recognizing disparities in policing and the uneven outcomes of the criminal justice system has led scholars to question how data is used to support data-driven policing. A growing number of critiques ask how problematic policing practices become embedded into data that is then fed into predictive systems (Richardson, Schultz, & Crawford, 2019). In an investigative study for ProPublica, Julia Angwin et al. (2016) revealed how recidivism risk software used in courts was biased against Black people. Many recent articles focus on how using biased data to train predictive software models used in policing will result in those biases becoming sedimented and replayed over and over (Robinson & Koepke, 2016; Jefferson, 2017; Minocher & Randall, 2020). Data, they argue, reflect the racist social structures from which they have been collected. In the context of growing public concern and awareness of the racist practices and outcomes of the police and justice systems, the integration of software into decision-making systems has attracted well-earned public scrutiny. Following Brian Jefferson (2020), recognizing the longstanding racist structures of policing to which technology connects is not to argue that tech companies are the cause of racist policing, but rather, to argue “that they capitalize on its ongoing legacy” (p. 9). While developers might distance themselves from overt racism in policing, any algorithmic augmentation of policing will become entangled with the inescapable presence of structural racism. But it is that very context that makes policing a lucrative possibility for technology companies.

Urban geographers have shown renewed interest in understanding how technology companies become embedded within urban governance through computation, big data, algorithms, and corporate visions of the “smart city” (Wiig & Wyly, 2016). As city governments increasingly adopt digital tools, they run the risk of translating “urban problems into technological problems, requiring technological solutions,” which are often detached “from the actual social relations that define urban life” (Alvarez León & Rosen, 2020, p. 501). While scholars have expressed concern over the opacity of the technologies used within urban governance, in this article I focus specifically on this detachment between the applications of technology and urban social relations. Following Fields et al. (2020), “a focus on the apparent opacity of platforms may reify them as external to, rather than thoroughly embedded in, the relations among devices, people, and the urban” (p. 465). In other words, focusing on data and algorithms might help understand the potentials of a particular technology, but situated social and material relations enable those technologies to exert power (Safransky, 2020). The power embedded in the so-called “smart city” is complex and shifting, made up of intersecting and often conflicting political and corporate interests, epistemologies, and visions of the future (Derickson, 2018). As urban geographers have shown, power expressed through digital urban governance often builds on and amplifies existing processes of racialization, whether expressed through policing (Jefferson, 2018), algorithmic market value assessments (Safransky, 2020), or predictive vacancy mapping (Noterman, 2021). Considering that the commodification of everyday life through big data is a lucrative and growing site of capitalist accumulation (Thatcher, O’Sullivan, & Mahmoud, 2016), urban spaces have become increasingly permeated with and governed by digital technologies.

¹ Recently, news outlets have begun aggregating data on police killings. The Washington Post, for example, keeps a database on fatal shootings by police since 2015: https://github.com/washingtonpost/data-police-shootings
As these digital technologies become increasingly routine, mundane, and embedded within the fabric of the city, their power becomes normalized and potentially depoliticized (Datta & Odendaal, 2019), which should raise serious concerns when they become part of policing. Geographers have shown how embedded sensors to detect gunshots (Shotspotter) (Cowen, 2020), online neighborhood groups (Nextdoor) (Bloch, 2021), private and public closed-circuit televisions (CCTVs) (Graham, 2002), and social media (Lally, 2017) have all aided and amplified racialized policing in urban spaces. As digital services proliferate, we can expect more of them to intersect with policing, sometimes in surprising ways. Elizabeth Joh (2019) argues, “artificial intelligence and robotics will lead not just to increased surveillance within a smart city, but the embedding of policing into the built environment” (p. 181) as police functions become automated, embedded within urban infrastructures, and managed through contracts with private software companies. Urban insights that these various technologies promise are often aggregated into real-time crime centers—forms of urban dashboards built to inform police operations (Mattern, 2015). Predictive policing becomes one of many possible software modules that can be integrated into these command centers. Juxtaposed alongside and sometimes combined with other algorithms and data, predictive policing is one of a proliferating number of technologies that aim to inform urban policing.

In order to examine the role of digital technologies in informing urban policing, I interrogate the processes through which predictive policing becomes integrated into infrastructures of governance. Research that centers problems of data and algorithms are important in critiquing predictive models, but they tell us little about how these emerging tools are put into use. As Emily Kaufman (2017) has argued in relation to stop-and-frisk practices in New York City, police practices might have little relation to insights provided by algorithmic black boxes. Instead, she argues, those practices might be nonrational and racist, “hiding behind a screen of algorithmic precision” (p. 6). Similarly, early social science studies of technical systems highlighted the need for interrogating technologies in their situated contexts—in use, embedded within social practices and relations (Suchman, Blomberg, Orr, & Trigg, 1999). The complex and often agonistic relationships that emerge between digital technologies, people, and institutions (Crawford, 2016) means that the implementation of digital technologies can be a fraught and unpredictable process. The discretion afforded to police officers in adopting and acting upon digital technologies combined with the difficulties in studying policing means that policing itself might be as much of a black box as predictive policing algorithms.

In this article, I draw from interviews with software developers and an analysis of related promotional, archival, academic, and media materials to examine the challenges of implementing predictive policing systems. Instead of a smoothly process of integration, the take-up of these systems is uneven and fraught, but most importantly, largely opaque to even those building predictive systems. The developers of predictive policing software are insulated from the everyday practices of policing—practices that are the target of transformation by that software. In this article, I argue that predictive policing in the United States is a modular technology, plugged into the black box of policing. It is modular insofar as it is developed in isolation from the practices it attempts to transform. This modularity mirrors modular logics of computer programming and has resonances with colorblind approaches to neoliberal governance (McPherson, 2018). As a result, the guiding premise of predictive policing, which centers on a model of deterrence, sits uneasily with the material practices of everyday policing. Additionally, modularity enables developers to deflect criticism away from the programs they build. And finally, modularity means that software can be reconfigured and connected to other systems,
which threatens to undermine the set of best practices that guide its development. In the next section, I outline a brief history of data-driven policing to help explain the widespread adoption of predictive systems into policing.

**Background**

The analysis of data has long been a part of policing, from the use of evidence in investigative research to the pinning of crime locations on printed maps to identify geographic patterns of crime. Beginning in the 1960s, some police departments began using computational models to forecast calls-for-service to assist in the allocation of patrol cars (Chaiken et al., 1975). As computers and geographic information systems (GIS) became more accessible, computational methods to automate statistical analyses of crime and map the results became more ubiquitous in police departments (for a longer history of the role of statistics and computation in policing, see: Jefferson, 2020). Computational analyses and modeling of crime statistics allow police departments to pinpoint high crime “hotspots” and target them with police patrols. A series of criminology studies, beginning in 1995, have consistently reiterated the effectiveness of combating crime through the targeting of hotspots, making it a widely adopted strategy in police departments. These studies came at a time when some scholars were arguing that, in its current form, policing did not prevent crime (Bayley, 1996). Hotspot studies were an important defense of statistical approaches to proactive policing at a time when commonsense understandings of the function of policing were cast in doubt. The uneven integration of systems of analysis and policing, however, introduced new problems and abuses into policing.

Rolled out in 1995 in New York City, CompStat, for example, formalized methods of crime data storage, analysis, and mapping for police departments. Hotspot maps produced by the CompStat system identifying concentrations of crime would inform the deployment of police patrols in the city. But as the collection of crime statistics became embedded within the everyday operations of the department, officers were incentivized to keep those numbers low. Because promotions and other rewards became tied to crime statistics, officers deployed a number of methods to make it appear that crime was decreasing within their beats, often by downgrading serious crimes to lesser offenses (Eterno & Silverman, 2010). So while some accounts credit systems like CompStat with significant reductions in crime\(^2\), how much those statistics reflect the department’s pressures to game the numbers (in addition to other structural factors at play) remains an open question (Eterno & Silverman, 2010). As departments increasingly turn towards data to inform daily operations, we can expect other complex entanglements of structures, practices, imaginaries, and software that belie the superficial simplicity that governance and evaluation through statistics might imply.

The use of software to produce data-driven policing insights has been spurred on and supported by the turn to proactive policing. Facing a crisis marked by declining public trust, increasing crime rates, and the inability to prevent crimes, police departments in the 1990s began to move towards proactive methods of policing (Committee on Proactive Policing, 2018). Instead of being a reactive force that only responded to emergencies and calls for service, this new method of policing called for strategic interventions that included hotspot mapping, community policing, broken windows policing, stop and frisks, focused deterrence, and problem-oriented

---

\(^2\) the NYPD’s website, for example, claims that CompStat “successfully drove down crime to record levels not seen since the 1950s”: https://web.archive.org/web/https://www1.nyc.gov/site/nypd/stats/crime-statistics/crime-statistics-landing.page
policing. Whether focused on individual offenders or geographic problem areas, these methods all rely on data to more precisely target people and places while generating more data through police interactions, interviews, and arrests.

Proactive methods have become firmly entrenched within the day-to-day operations of police departments—new software packages promise to more efficiently and effectively hone these methods, often backed by claims of scientific methodology and objectivity (Ferguson, 2017). With policing once again facing a public crisis of legitimacy driven by police violence, killings, and cases of widespread corruption within police departments, this veneer of scientific objectivity can be perceived as a way to mitigate officer bias in policing decisions. Software simultaneously promises cost benefits for underfunded departments, making it easier for officers to more efficiently carry out police work and distribute resources (Perry, McInnis, Price, Smith, & Hollywood, 2013). Efficiency here entails the precise targeting of places and populations, which often means being in the right place at the right time to effectively fight or deter crimes (whether or not strong evidence of the effectiveness of these methods exist). Bolstered by academic partnerships with police to study crime patterns, federal government funding earmarked for technology acquisition, and constantly improving technology, computational methods were easily integrated with proactive policing (Ferguson, 2017). The move to a proactive ideology of policing, then, incentivizes data-driven targeting and preemption of crime.

With the turn to computational methods comes the increased need for specialized technical positions within police departments. Many departments today rely on crime analysts trained in GIS to store, analyze, and map crime data and inform policing tactics and deployments. ArcGIS software has a range of applications and modules specifically tailored for crime analysis work, including hotspot mapping. Additionally, ArcGIS’s parent company Esri advertises multiple events, tutorials, white papers, videos, and other promotional material related to crime analysis on their website. The turn to hotspot mapping and other computational approaches to crime data was only the beginning of an ever increasing adoption of software by police departments, often supported by GIS methods and software.

If early data-driven approaches to crime using software analyzed existing geographic distributions of crime, more recent efforts have sought to predict or forecast where crime is most likely to happen in the future. Often called predictive policing (although many developers prefer to say they “forecast” crime instead of “predict” it), this mode of computational analysis uses crime theories and historic crime data to model crime in both time and space to produce dynamic and probabilistic understandings of crimes that have not yet occurred. Used almost exclusively in urban areas because of the need for dense data, predictive software will recommend officers patrol selected areas during their uncommitted time. These geographic approaches to predictive policing, which are the subject of this article, have important implications for how space might be understood and governed by police forces. In the United States, predictive systems are often built by private companies and customized to the needs of urban police forces. In contrast, in the United Kingdom, systems are largely built by academics who work with police forces in exchange for access to data. Public-private distinctions, however, are blurred in both contexts. The private, U.S.-based PredPol, for example, was founded by a UCLA professor and has been

---

4 Predictive policing can also be used to target individuals to determine their likelihood of committing crimes in the future. For example, the Chicago Police Department produces a Strategic Subject List (SSL) of individuals determined to be at risk of committing future crimes by analyzing data on crime, social network, and other indicators with questionable results (Saunders, Hunt, & Hollywood, 2016).
tested in the U.K. context. Private systems like PredPol and Shotspotter Missions (formerly Hunchlab)—both in widespread use around the U.S.—build on theories and algorithms developed by academics in the U.K. In this article, I use interviews and materials drawn from both the U.K. and U.S. theorize the implications for the integration of software into policing in the United States.

While critical scholars have expressed numerous concerns with the data used in algorithmically-driven policing, fewer critical studies have examined how systems integrate with existing infrastructures and practices (for notable exceptions, see: Brayne, 2017; Jefferson, 2017; and Shapiro, 2019). This opacity is not just the result of an understudied area of concern, but, as I argue below, related to the structures of policing and the mode of integration of predictive software. Software’s impacts on the concrete practices of policing is similarly opaque to software developers who work closely with departments to integrate their products into infrastructures of policing. Developers can only glimpse the impacts of their work through the narrow lens of geospatial data, periodic randomized controlled trials (RCTs), or the occasional visit to a department, as the modular integration of predictive systems obscures what can be known about policing.

“It makes almost no difference which algorithm you use”

Drawing on interviews with and observations of software developers from 2017–2018 and an analysis of promotional materials, academic articles, and popular media, I argue that predictive policing is insulated from the practices it attempts to transform. This insulation is the result of internal and external pressures that fortify the separation between the world of data and the concrete practices and social relations from which that data is abstracted. This gap is significant considering that the stated purpose of predictive policing is to intervene in and change the data it models. In other words, predictive policing aims to not only predict crime, but also prevent future crimes, thus intervening in the data patterns it analyzes5. These interventions require effective means to integrate software into the practices, routines, and decision-making processes of policing. But, as I argue, these processes of integration are fraught, producing doubt amongst developers—doubt that illustrates the gap between the world of predictions and the world of policing.

In contrast to the bold claims of data-driven accuracy through which predictive policing is advertised, a recurring theme in my interviews with developers was a recognition of the difficulty in translating predictions into policing practices. As one developer explained, “It makes almost no difference which algorithm you use, what matters is how the police turn [predictions] into actionable plans.” Another observed, “there is an increasing focus on accuracy and I think it’s in some ways misplaced. As long as you have a decent level of accuracy, I think incremental changes don’t really matter too much.” Statements like this point to a fundamental difficulty in translating predictions into effective policing strategies. Solely focusing on the accuracy or fairness of models would miss the subsequent difficulties inherent in translating models into practice. Open to interpretation and integrated differently into police departments, the process of translation is an important part of the necessarily tightly-coupled systems of algorithmic governance.

So while developers I spoke with are able to tout the accuracy of the models they build while defending their choices of data, they spoke less confidently about policing. On the one

5 The contradictions that arise from the simultaneity of prediction and intervention has been used to critique the effectiveness of predictive systems (Andrew G Ferguson, 2017; Shapiro, 2019)
hand, this hesitancy sometimes resulted from a recognition of the uneven and problematic practices of policing. For some developers, predictive policing offered the possibility of a fairer, more scientific approach to crime data, which could help mitigate some of this unevenness. On the other hand, hesitancy was sometimes indicative of the gap separating models and practices. Models can be verified by developers, but the messy world of social relations and practices often evades such scrutiny.

**Facing the blue wall**

The everyday practices of policing are notoriously difficult to study. As Mat Coleman (2016) argues, the “blue wall” that shields police practice is a formidable obstacle to studying the police, both qualitatively and quantitatively. He writes, “there is something perversely uneventful and chronically disappearing about police work which makes it exceptionally hard to excavate and interrogate” (p. 77) as interviews become public relation events, observations do not disclose much, and power is forever disappearing. Quantitative measures of policing—which are the primary way developers can see the results of their work—can only give foggy accounts of the unevenness of policing, while further abstracting from how power plays out on the ground (Coleman, 2016; Woodward, 2016). Despite hopeful and often imaginative claims for how predictive policing can transform policing practices, those who are involved with the production of such tools face a similar “blue wall” that limits their knowledge of how software is actually integrated into everyday practices. Resistance to changing practices within police departments is not a problem that only applies to technology, but plagues other efforts to introduce evidence-based practices to policing (Sherman, 2015). In North America, efforts to introduce evidence-based practices into police departments have mostly failed (Kalyal, 2019). Considering that “…technology will not be used in evidence-based ways if an agency’s approach to policing more generally does not involve evidence-based policing” (Lum & Koper, 2017), we should be suspicious of narratives that assume a frictionless integration of technologies that aim to reform policing.

Attempts at police reform meet the everyday and dispersed resistance of the blue wall, which is sometimes revealed to developers when they meet with officers to test products. Two developers I interviewed, for example, described ride alongs they conducted with officers in a major U.S. city to observe how they were using their predictive software. Both found the experience illuminating as it illustrated the concrete difficulties of integrating software into existing policing practices. They both described how experienced officers expressed skepticism about the software and during ride alongs showed no intention of using it. As one developer told me, an officer on a ride along made no effort to use the software, even though testing it was the point of the ride along. Instead, he displayed his deep knowledge of his police beat. “He’s been there for twenty years and he just knows this thing like the back of his hand,” described the developer. “and he almost… seems like a psychic when you’re going around with him. He’ll be like, ‘all right I’m gonna go up this block, and then you see that person there, now if we go around on this other block he’s gonna be there…roll down your windows a little, he’s gonna say this thing as we pass.’” The predictive capacity of software, in this instance, is met with the predictive abilities of the seasoned officer whose intuitions and knowledge of his beat is used as a mode of resistance to data-driven technological augmentation. The sedimented practices of policing as it always has been done runs up against attempts to shift those practices, here
exposed as a fleeting glimpse into how software might be summarily ignored even after being integrated into a department.

In another description of a ride along, a developer described how an officer ignored the predictive policing map because it usually just confirmed what he already knew, exposing a recurring problem that influences how software is built. Developers explain that software needs to display predictions that make sense to officers, which convinces them that it “works,” while also revealing new insights about the world, to show that the software adds value and helps reveal new insights about crime (Shapiro, 2018). The need for software to fit officer expectations while shifting them slightly severely limits the possibilities for software to fundamentally shift police practices. In the above case the officer discounted the software since it showed what he already knew, while he ignored those predictions that he did not understand. This led him to not feeling the need to patrol in the way prescribed by the software since it merely revealed what was obvious. In her work with the LAPD, Sarah Brayne (2017) found similar resistance to predictive technologies, as officers often claimed that they already knew where crime as going to happen. She theorizes that technologies face resistance by officers, in part, due to fears of managerial surveillance and deskilling of the profession. Owing to the fact that policing is already notoriously difficult to study, these glimpses of resistance to software raise important questions for the possibility of software substantively changing policing practices in ways envisioned by software developers especially considering the obdurate structures and culture of police departments.

**Predictive policing and modularity**

In order to integrate predictive systems, developers write and communicate best practices for their software, often centered on deterrence. But once they hand off software to a department, they have little say in how it is used, beyond making recommendations that may or may not filter through chains of command. How the insights provided by software are interpreted and acted upon, or summarily dismissed, is largely opaque and context-dependent. While the algorithms that produce such insights have received considerable attention, it is likely that the translation between predictive software and policing practices is the more significant occluded relationship that haunts the implementation of predictive systems. While scholars have been able to recreate and experiment with predictive policing algorithms (for example, see: Lum & Isaac, 2016, where the authors use a PredPol algorithm published in an academic journal and train it on drug arrest data), studying how officers actually use software is a more ambitious and fraught undertaking. This is due in part to the blue wall of policing, but also because of the individual discretion afforded to officers in using, interpreting, and acting on software (Brayne & Christin, 2020), which we would expect to differ according to local contexts, police organizational structures and cultures, and receptiveness to data driven and evidence-based practices.

On the one hand, predictive systems ingest crime data produced through complex and uneven systems of policing, incident reports, calls-for-service, and social processes. On the other hand, algorithmic systems filter and analyze these data to make recommendations for the spatial and temporal distribution of police while sometimes even recommending strategies police should deploy. But these processes, while intimately connected to practices of policing, also stand apart from them, insulated from that which they claim to transform. In other words, the analysis of crime data is bracketed off from the specificities of policing practices, beyond the generalized assumption that police presence in the right place at the right time will deter crime from
happening\textsuperscript{6}. But police practices are not the only phenomena bracketed out from consideration. Despite some popular claims to the contrary, known predictive systems do not use arrest data in recognition that this would cause a feedback loop that would only entrench existing policing practices. Similarly, drug violations are considered to be largely police driven and considered by most inappropriate for use in predictive software. And, significantly, race as a variable is never used so software vendors can claim a colorblind approach to fighting crimes as geographical differences in crime rates occludes racial difference.

Tara McPherson (2018) connects the colorblind logic of post-Civil Rights era neoliberalism with the development of modular logics in computer programming. Both, she argues, are methods to reduce complex systems to smaller, discrete parts. This modular approach creates ways of dealing with systems that are resistant to intersectional thinking. In the case of computer software, programmers can design discrete, modular functions that can be plugged into a main program, abstracting them from each other and the functioning of the machine (Chun, 2011). The obfuscation of code into discrete modules works to black-box “messy internal details, thus masking technical, organizational, cultural, and political conflicts to display only a consistent interface” (Russell, 2012, pp. 257–258). Reducing modules to inputs and outputs while obfuscating their internal operations also allows for labor specialization and division as programming becomes a series of discrete problems that need not intersect (Galloway, 2006; Russell, 2012). Similarly, colorblind and modular thinking means a city can be reduced to “a map of derelict zones and urban blight that computation could isolate and contain,” whether through divestiture or policing without considering of race, structural inequality, or other forms of difference (McPherson, 2018, p. 64). Both forms of modularity make it difficult to think systematically across difference to understand the intersecting structural forces that, for the purposes of this study, produce understandings of crime and methods to fight it through policing.

While McPherson does not claim a direct, causal relationship between the rise of modular programming and the bracketing off of race in colorblind policies, she shows how they were produced in parallel, echoing the logic of each other. In predictive policing, modular thinking in regards to computation and race intersect in consequential ways. On the one hand, we find a very explicit expression of modularity as race and other categories of difference are bracketed out from consideration. The category of “crime” and how it might be addressed are treated as independent of racial and other markers of difference, even if it is clear that the force of law as expressed through policing and the justice system exploit, reify, and amplify existing forms of difference\textsuperscript{7}. So while software is quite good at working with the data it is given, making impressively accurate predictions into the future, the fraught categories of difference are removed from consideration. On the other hand, software can then be plugged into the black box of policing with little actual knowledge of how the two interact and function together. This, I argue, parallels the modular logic of computer programming as described by McPherson, where one function need not know how another works in order to be plugged in. Developers of predictive policing can write recommendations for best practices in using their software and

\textsuperscript{6} Almost all of the developers I talked to centered their understanding of policing on this premise. One developer, however, observed: “it’s a completely unknown question about whether police patrol actually prevents crime, in any sense other than you’re literally standing there when a crime is going to happen and you prevent that.”

\textsuperscript{7} There have been some recent efforts to create systems that take the potential harm of over-policing in minority or low income communities into account when allocating patrols, but they remain theoretical at this point. They are also only able to modulate the amount of policing in particular places or against particular people, which does not signal a significant change to policing as such, and will likely meet resistance by police departments.
produce imaginaries of how policing functions, but the blue wall of policing separates the module of mapping software from the everyday practices of policing.

In what follows, I highlight three tensions that arise from the modular approach to technological integration and their implications for thinking beyond the algorithms of policing. First, I show how understandings of deterrence sit uneasily with the actual practices of policing. Second, I show how the separation of data and practices of policing can act as a defense of predictive systems. And finally, I argue that the modularity of software means it can be misused in ways that undermine the best practices that guide its development.

**Tracing modularity**

Software developers narrate their tools as producing crime deterrence effects, but how the police interpret and react to predictions is largely unknown and likely undermines such simplistic understandings of policing. In an academic paper, which includes two of the founders of PredPol among its co-authors, researchers deployed an RCT to determine if PredPol leads to racially-biased arrests (Brantingham, Valasik, & Mohler, 2018). Recognizing that racial disparities in policing are rampant (citing 27 studies), the authors tested to see if racial biases were heightened in areas that software had marked as high risk. While overall arrests were not affected, arrests in areas that were marked by software increased significantly. Additionally, racial disparities in arrests remained unchanged as arrest rates rose across the board in predicted areas. The authors hypothesize that arrests increased due to predictive policing software being more effective at predicting crime than existing policing practices, citing their own academic study of the software they built and sell, which happens to be one of the few studies that has shown predictive policing is effective in reducing crime (Mohler et al., 2015). The findings are significant because they undermine the idea that predictive policing will lead to deterrence without increasing arrests rates. Instead, according to this study, software geographically targets predicted areas for increased arrests while maintaining existing arrest disparities. This finding is consistent with studies of other targeted enforcement interventions, which tend to drag residents into the court system for reasons other than those of the interventions (Goldkamp & Vlcic, 2008).

The potential for predictive policing to redistribute police violence is central to many critiques of the technology. This is a concern shared with developers who claim their technologies are premised on deterrence. In promotional materials, training guides, and discourse, software companies insist that crime predictions are not probable cause for stops and arrests. As Andrew Ferguson (2017) has argued, how predictive policing factors into reasonable suspicion or probable cause judgments that would justify a police stop remains legally unknown.

---

8. the discretion afforded to officers in day-to-day operations begs the question of how much RCTs influence officer compliance with the systems being tested and how that compliance might change over time.
9. this was communicated to me through interviews and is evidenced in official materials: including: https://www.muckrock.com/foi/elgin-7770/foia-elgin-police-dept-predpol-documents-51858/#file-190432: “High crime areas may be grounds for further investigation, but additional objective evidence must always accompany reasonable suspicion and probable cause.”; https://web.archive.org/web/20201112032501/https://www.predpol.com/5-common-myths-predictive-policing-predpol/: “The presence of police officers in the prediction areas creates a deterrence and suppression effect, thus preventing crime in the first place.”; and https://web.archive.org/web/20171209232225/http://robertbrauneis.net/algorithms/HunchLabACitizensGuide.pdf: “We are forecasting risky locations for crimes to occur, with the goal of no one being arrested because the crime is prevented.”
In the Supreme Court ruling in Illinois v. Wardlow (Rehnquist, 2000), for example, the fact that a person was in a “high crime area” was deemed to be, in part, admissible evidence for police to determine reasonable suspicion and stop a suspect. In over policed communities, a person being in a “high crime” area is often used as a justification for unwarranted stops and searches, often targetting people of color (Kaufman, 2016). Ferguson (2017) argues that predictive policing creates mini high-crime areas in which “police may feel additional license to investigate more aggressively” (p. 79). Whether or not this increase of scrutiny driven by predictive policing violates people’s 4th Amendment rights against unreasonable searches and seizures remains legally untested and will depend on how Illinois v. Wardlow is interpreted in regards to crime predictions.

Regardless of the constitutionality of stops within a predicted crime zone, the PredPol RCT shows how the intent of predictive policing (crime deterrence) is transformed in use (resulting in arrests). While the authors of the study cite increased crime rates as a cause, this claim demands further scrutiny. In a promotional video, PredPol’s competitor Hunchlab warned that there was only a 1–2% chance of a predicted crime occurring in the space and time frame of the prediction. In the case of the PredPol RCT, crimes predicted were “burglary, car theft, and burglary theft from vehicle.” Assuming that the PredPol algorithm is similar in accuracy as Hunchlab’s and that there is some crime deterrence effect of officer presence, it is unlikely that many arrests are related to the crimes being predicted. Considering that over 80% of police arrests are for minor offenses (Lum & Koper, 2017) and police rarely solve the types of crimes that form the basis for the RCT’s predictions (Baughman, 2020), the effects of predictive policing seem at odds with its intent. While additional data would be needed to understand what happened in the RCT, we can assume that the police are effectively engaging in broken-windows policing in predicted areas, targeting people for minor offenses. If this assumption is true, this means that the same crimes that are deemed unreliable for use in predictive systems because they are officer-initiated become targets for police interpreting those same predictions.

Developers recognize potential problems with policing that might arise once their software modules are plugged into policing, but the separation between their work and the practices of policing leave them with few means to address these concerns. The developers of one software system who I interviewed, for example, decided to limit information about crime predictions available to patrolling officers. This change was in direct response to potential 4th Amendment violations. Developers reasoned that a box showing a high likelihood of a particular crime happening could lead to reactionary policing of people in those boxes. Instead, as they argued, the box only leads an officer to patrol a particular area, thus producing a deterrence effect. By tweaking what information is available, developers hope police practices will be nudged towards the intended uses of predictive policing, even if they are largely shielded from such information. Another developer told me about the ethical dilemma caused by a police request for manual overrides of their software. The development team was able to push back against the request, adding some friction in the software to limit manual overrides. For one

10 now owned by ShotSpotter and rebranded as “Missions”
11 Hunchlab claims higher accuracy than its competitors because of its use of machine learning trained on many variables. In contrast, PredPol uses only three variables: “crime type, crime location, and crime date/time” (see: https://www.predpol.com/) using a modified earthquake aftershock model. While it is not my intent to evaluate these claims, here I assume they have similar accuracy.
12 A PredPol training manual, released through an open records request, controversially suggested a broken-windows approach as one way to use their software: https://www.muckrock.com/foi/elgin-7770/foia-elgin-police-dept-predpol-documents-51858/#file-190432
developer I spoke to, negotiations to determine how features are implemented was an important part of maintaining a sense of agency in recognizing and limiting potential ethical problems with software as it is put into use. It is an illustration of the ambivalence of developers as they produce tools that they believe can contribute to making the world a safer and fairer place through deterrence, while recognizing the profound problems of policing that threaten to undermine those goals.

Since the modularity of predictive policing software leaves developers little room to directly address policing practices, this often leads them to imagine how officers might interact with the software and its features. In development team meetings I have attended, stereotypical user groups are imagined by developers to understand how a new software feature might be used. These groups might include officers who are receptive to software, not interested, or absent-minded, with each establishing a different relationship to predictive systems, which in turn produces different outcomes and practices. In imagining users, developers attempt to identify with the everyday practices, concerns, proclivities, and feelings of officers in the field in an attempt to bridge the gap that separates the functioning of software with how users actually use it. When testing new features, developers told me that they will sometimes get into their cars and pretend they are police, allowing the software to lead them to places of increased risk and patrol as prescribed. As one developer told me, when writing code it can be difficult to know things will play out in practice, so using the software is a means to develop spatial awareness of particular use cases and, in turn, make software features more usable. Imagining themselves as officers might give developers some insight into how to make software more usable or approachable, but this attempt to bridge the gap produced by modularity can do little to address the violence work that is central to policing.

While the gap between the stated intent of predictive policing and actual police practices can sometimes be frustrating for developers, it can also be deployed strategically to defer responsibility away from software. If the stated goal of predictive policing is to change police behavior, modularity simultaneously allows developers to distance themselves from bad behaviors. Jeff Brantingham, a co-founder of PredPol, argued in response to concerns of bias: “An algorithm is not going to get out of the car and police the problem… Police get out of the car and police the problem and as a result they have to police constitutionally” (DeGeurin, 2018). Prescribing a set of best practices centered on deterrence while remaining removed from the concrete practices of policing allows developers to deflect criticism.

The ability of developers to deflect criticism extends to their use of data, which has been the focus of numerous critiques of predictive policing software. As mentioned above, developers leave out racial data from their systems, allowing them to claim a colorblind approach to crime prevention. While popular critics often pose developers naive subjects who use problematic data that creates racialized feedback loops, developers quickly dismiss these critiques. Drawing from criminology literature, developers defend their data choices by pointing out that they use a combination of major crime types that are well-reported (like homicide and burglary) while drawing from calls for service in cases of crimes that could be drive by officer presence. Of course, this does not exhaust the possible problems with predictive systems, but can serve as an easy defense against critiques that seem to misunderstand the thought that goes into producing these software systems. Bracketing off certain types of data from consideration—which parallels modular approaches to urban issues in a colorblind, neoliberal approach to governance—becomes an easy line of defense against many forms of criticism. Additionally, this more evidence-based approach, rooted in criminological research, is easily contrasted against existing
approaches to policing, which often rely on unchanging hotspot maps and officer intuition. Plugging a predictive system into policing, as the argument goes, might just nudge police practices in the right decision. Although what they do when they get there, if they get there, might just result in a redistribution of violence and harassment.

The belief in predictive systems nudging policing in the right direction relies on the faith that systems will be used as intended, but with modularity comes the possibility for untold abuses. Making software adaptable to different policing contexts is a central concern for vendors who want to sell their software to police departments with different needs, practices, cultures, and workflows. To do so, software is produced to be reconfigurable in its implementation and interoperable with other software and data. So while developers will address ethical issues by prescribing what kinds of crime data is appropriate to model, how patrols should be conducted, and how software should integrate within departments, the fluidity of software means all of these normative suggestions can easily be undermined by those who use the software. For example, reconfigurability in software allows for users to incorporate their own data into models—data that may or not meet the ethical standards of either developers or the criminology literature they draw from. Adding unethical data, however, might fit into current departmental practices and appear to be effective within the context of crime data, which we know to be overdetermined by intersecting social, economic, and political structures.

Adding to concerns over misuse are the ways that software is casually talked about when being promoted or sold. For example, developers will openly talk about how the addresses of parolees and others recently released from prison could be incorporated into existing models. Or, conversely, models could guide recidivism decisions by analyzing the crime risk of a particular area to which a prisoner is released. One developer, in discussing the ethical questions faced in developing predictive policing, explained “how dangerous it can potentially be in the wrong hands,” if, for example, “you do it the wrong way and come up with some Draconian vision.”

Even without misusing data, problems arise in how predictions are implemented and acted upon. One developer described how Immigration and Customs Enforcement (ICE) could use existing predictive policing software to target undocumented immigrants who get robbed because they carry cash, switching the purpose of the software away from protecting people to targeting people. The reconfigurability of software facilitates the addition of any data, whether or not it meets some ethical criteria, while its modularity allows it to be easily integrated into other software systems through API calls. ShotSpotter\(^{13}\), license plate readers, CCTV cameras, and other kinds of surveillance technologies can, and sometimes do, become integrated with place-based predictive policing systems, compounding potential issues with software. In the isolated conditions of the software laboratory, ethical problems can be summarily addressed and dismissed, but once integrated into the messy and amorphous world of policing practices, technological systems, and messy data, software opens up to a fraught field of intersecting oppressions and abuses that exceed the accounting abilities of software developers. Deferring responsibility becomes a key survival strategy for software vendors, but reaches its limits when met with the unresolved voids in discourses and practices.

\(^{13}\) since buying Hunchlab, ShotSpotter has integrated it with their gunshot detection technology: https://web.archive.org/web/20210308152857/https://www.shotspotter.com/law-enforcement/patrol-management/
Conclusion

While many critics have expressed certainty in the racist effects of predictive policing, the complexities of how these systems integrate with existing data, practices, and imaginaries leads to myriad possibilities for integration. At its worst, predictive policing will spatially entrench existing oppressive practices of policing. At its best, it might move otherwise uncommitted police away from unchanging hotspots, offering temporary reprieve for over-policed communities. But any spatial shifts in policing, at least within the context of policing in the U.S., will likely only redistribute the harm and violence central to policing (Seigel, 2018; Shapiro, 2019) in complex and unpredictable ways. For example, we should not assume that the demographics of a neighborhood are indicative of who might be targeted by the police. In drug enforcement, for example, police “tend to target suspects whose race is incongruent with the neighborhood racial context” (Gaston, 2019). Without a concerted effort to shift policing to a model centered around deterrence without stops and arrests—a shift that would be unprecedented within U.S. policing—any shift in the spatial distribution of police does little to address the problems central to policing.

I began this article with a brief history of these problems in order to contextualize the structures into which predictive policing attempts to integrate. When studying technology it is important not to underestimate the obdurate nature of existing structures and overestimate the ability for technologies to shift the practices that make those structures possible. In theorizing predictive policing as a modular technology, I have shown how the difficulties of integrating predictive software reveals the resistance of the police to evidence-based practices and reform. Modularity also reveals how developers are able to exploit the gap between their work and its implementation as a means to deflect criticism. Finally, I argued that modularity opens predictive policing up to untold abuses as numerous data and functions can be plugged in and mixed together for questionable purposes.

The relative autonomy granted to police departments and the discretion afforded to individual officers coupled with a general lack of accountability means that how policing interacts with new technologies will likely be an evolving relationship. In some contexts, we might expect crime statistics to be the target of manipulation, as scholars have observed in particular implementations of CompStat. In other contexts, predictive policing might be largely ignored, used as a marketing tool that does little to change concrete practices. In a more positive vision, it could encourage departments to center practices of deterrence, thus avoiding the worst excesses of policing that disproportionately target and imprison the most vulnerable. This last vision, however, is probably unrealistic as it relies on a revisioning of policing as it exists in the U.S. This revisioning would likely require other sorts of desires, allegiances, and social movements that exceed the capabilities of a technology that can only be plugged into existing, reform-resistant systems. In the end, predictive policing’s most enduring contribution might not be its ability to change policing, but rather, in its ability to show how policing resists change, which might lead us to imagine other ways to organize the spaces of the city.
References


Lane-McKinley, Kyle, Tsungmey, Tenzin, & Roberts, Laura Weiss (2018). The Deborah Danner Story: Officer-Involved Deaths of People Living with Mental Illness. *Academic Psychiatry*.


