Cops, Docs, and Code: A Dialogue Between Big Data in Health Care and Predictive Policing

I. Glenn Cohen[†][*] *& Harry S. Graver*[**]

TABLE OF CONTENTS

"Big data" has become the ubiquitous watchword of this decade. Its meaning is somewhat protean, but from the business side it is usually thought of as consisting of the "three V's" — Volume (vast amounts of data), Variety (significant heterogeneity in the type of data available), and Velocity (speed at which a data scientist or user can access and

[*] Professor, Harvard Law School. Faculty Director, Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics. We thank Andrew Crespo, W. Nicholson Price II, and participants at the Harvard Law School Health Law Policy, Biotechnology, and Bioethics Workshop for helpful comments.

[**] JD Candidate, Harvard Law School.

analyze the data).[1] Some would add a fourth "V" of Value (the idea that big data would allow us to make valuable improvements to commercial or social systems).[2] On the legal side, perhaps the best definition comes from Julie Cohen who defines big data as the combination of a technology with a process — the technology "is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times" while the process "involves mining the data for patterns, distilling the patterns into predictive analytics, and applying the analytics to new data."[3]

Predictive analytics, which is something we want to do *with* big data, is "the use of electronic algorithms that forecast future events in real time."[4] It is very easy to be drawn into the exceptionalism of big data and its lingo — a result, no doubt, of the many business interests trying to "sell" the marketplace on expensive investments in big data.[5] Much of what "predictive analytics" conceptually does, however, is surprisingly quotidian. After all, when one decides between the chicken tikka masala or the baingan bharta at one's favorite Indian restaurant, the choice is in part guided by all sorts of data from past experiences (How filling? How spicy? How much gas later in the evening?).

The use of big data for predictive analytics is different along both a scalar and, in some cases, categorical dimension. On the scalar dimension, what is exceptional is the size and variety of data that can be harnessed to predict a future event and the speed at which one can do so. Imagine basing your Indian food choice not on your recollection of the last few dining experiences but on the combined experience of every patron of the establishment, those of 50,000 other Indian restaurants (sorted by age, race, gender, demographics), as well

[1] *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 4 (2014), https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf.

[2] *E.g.*, D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129, 1140 (2016).

[3] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1920 (2013).

[4] I. Glenn Cohen et al., *The Legal and Ethical Concerns That Arise from Using Complex Predictive Analytics in Health Care*, 33 HEALTH AFF. 1139, 1139 (2014) [hereinafter Cohen et al., *Legal and Ethical Concerns*].

[5] *E.g.*, Tim Harford, *Big Data: Are We Making a Big Mistake?*, FIN. TIMES (Mar. 28, 2014), http://www.ft.com/cms/s/2/21a6e7d8-b479-11e3-a09a-00144feabdc0.html#axzz30tH6hAOd ("As with so many buzzwords, 'big data' is a vague term, often thrown around by people with something to sell.").

as historical data on the fluctuating quality of key ingredients by region and 700 other data sources.

The categorical difference relates to machine learning and interpretability. Many, but not all, predictive analytics approaches rely on some form of machine learning. Most typically, with predictive analytics "a machine has been 'trained' through exposure to a large quantity of data and infers a rule from the patterns it observes," thereby learning input-output pairing from example rather than through a purposive human rule building approach.[6] The ability of machines to teach themselves adds another layer to the question of whether the prediction process is "interpretable" by people. That is, "a non-interpretable process might follow from a data-mining analysis which is not explainable in human language."[7] If asked by a court to explain how this kind of system arrived at a particular determination, it could be thus very difficult and sometimes impossible to do so. For this reason, some have referred to this as "black box" decision-making.[8]

Predictive analytics is interfacing with the law in a myriad of settings: how votes are counted and voter rolls revised, the targeting of taxpayers for auditing, the selection of travelers for more intensive searching, pharmacovigilance, the creation of new drugs and diagnostics, etc.[9] In this symposium paper, we want to engage in a bit

[6] Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 679 (2017).

[7] Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1519 (2013).

[8] *See, e.g.*, Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, 3 BIG DATA & SOC'Y 1, 1-2 (2016) (distinguishing three kinds of opacity related to machine-learning: "(1) opacity as intentional corporate or institutional self-protection and concealment and, along with it, the possibility for knowing deception; (2) opacity stemming from the current state of affairs where writing (and reading) code is a specialist skill and; (3) an opacity that stems from the mismatch between mathematical optimization in high-dimensionality characteristic of machine learning and the demands of human-scale reasoning and styles of semantic interpretation"); W. Nicholson Price II, *Big Data, Patents, and the Future of Medicine*, 37 CARDOZO L. REV. 1401, 1404 (2016) [hereinafter Price, *Big Data, Patents*] ("Black box medicine is 'black-box' precisely because the relationships at its heart are opaque — not because their developers deliberately hide them, but because either they are too complex to understand, or they are the product of non-transparent algorithms that never tell the scientists, 'this is what we found.' Opacity is not desirable, but is rather a necessary byproduct of the development process.").

[9] *E.g.*, Efthimios Parasidis, *The Future of Pharmacovigilance: Big Data and the False Claims Act*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS (I. Glenn Cohen et al. eds., forthcoming 2018) (manuscript at 111-26) (on file with authors); Cohen et al., *Legal and Ethical Concerns*, *supra* note 4; Kroll et al., *supra* note 6, at 636; Price, *Big Data, Patents*, *supra* note 8, at 1403-05.

of legal arbitrage; that is, we want to examine which insights from legal analysis of predictive analytics in better-trodden ground — predictive policing — can be useful for understanding relatively newer ground for legal scholars — the use of predictive analytics in health care. To the degree lessons can be learned from this dialogue, we think they go in both directions. As is typical of symposium articles, this piece self-consciously asks more questions than it will answer.

Part I briefly summarizes the main themes from the predictive policing legal literature before it very briefly turns to describing the emerging literature on predictive analytics in health care. Part II, the heart of the Essay, examines what can be learned from juxtaposing the two settings. A conclusion distills some lessons. This article focuses almost exclusively on the U.S. experience with both kinds of data use, leaving examination of lessons from international comparisons to other works.

I. ~~EVERYTHING~~ SOME THINGS YOU WANTED TO KNOW ABOUT PREDICTIVE ANALYTICS IN POLICING AND HEALTH CARE IN FEWER THAN 1700 WORDS.

A. Predictive Policing

Predictions are everywhere in our criminal justice system. When determining bail, judges evaluate the likelihood that a defendant will come back to court,[10] and estimate the chance that an individual will commit another crime before deciding sentencing. From the days of red pushpins on a board, police departments have similarly tried to forecast behavior. On the ground, these sorts of predictions require the judgment, discretion, and experience of officers. In *Terry v. Ohio*,[11] the Supreme Court phrased this sort of inquiry as: "[W]ould the facts available to the officer at the moment of the seizure or the search 'warrant a man of reasonable caution in the belief' that the action

[10] There has been increasing media and academic attention to the use of predictive algorithms in bail. *See, e.g.*, Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, N.Y. TIMES, May 2, 2017, at A22; Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. The programs referred to in these articles raise some of the same issues we discuss with policing — namely, the relationship between discretion and automated decisionmaking, as well as considerations about potentially disparate impact of predictive analytics's application — but are largely outside our immediate focus.

[11] 392 U.S. 1 (1968).

taken was appropriate?"[12] Recently, predictive analytics arrived at through the use of big data have radically expanded the sort of information available to police departments and officers. Typically, this revolution is referred to as "predictive policing."

Predictive policing is "the application of analytical techniques — particularly quantitative techniques — to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions."[13] Departments across the country are using a wide variety of these programs to shape crime prevention strategies. For instance, Shreveport's PILOT program attempts to identify future crime spikes a month in advance by analyzing past crime data against seasonal patterns.[14] Santa Cruz employs an algorithm that analogizes crime patterns to earthquakes, directing officers to 500 x 500 foot areas determined to have the highest chance of immediate crime.[15] In general, what makes "predictive policing" different from earlier police practice is not the use of quantitative data,[16] but the scalar and categorical elements discussed above — the sheer scope of the data available to law enforcement, coupled with rapid advances in machine-learning and analytical methods.[17]

Law enforcement agencies currently have access to massive and readily expanding amounts of data. Consider federal "fusion centers," essentially hubs of data collection for local, state, or national agencies, created for intelligence sharing purposes after 9/11.[18] Fusion centers aggregate and survey "public- and private-sector . . . reports, drivers' license listings, immigration records, tax information, public-health data, criminal justice sources, car rentals, credit reports, postal and shipping services, utility bills, gaming, insurance claims, data-broker dossiers, and the like."[19] Furthermore, police departments increasingly rely on third-party data aggregators to supplement their analysis with private information such as commercial buying patterns.[20]

[12] *Id.* at 21-22 (citing Carroll v. United States, 267 U.S. 132 (1925)).

[13] WALTER L. PERRY ET AL., PREDICTIVE POLICING: THE ROLE OF CRIME FORECASTING IN LAW ENFORCEMENT OPERATIONS 1 (2013) (ebook).

[14] *Id.* at 64-67.

[15] *See* Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 44-45 (2014).

[16] *Id.* at 43.

[17] *See* Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 873 (2016).

[18] Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1443 (2011).

[19] *Id.* at 1451.

[20] *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163

With this information, police departments use analytical techniques to make two sorts of predictions: *where* crime will happen and *who* will commit a crime. In targeting locations, police attempt to identify high-risk areas through a combination of historical crime data and current environmental vulnerabilities.[21] Models generally attempt to either calculate the extent that crimes will repeat around similar places ("near-repeat theory") or evaluate the factors that lead to criminal behavior and predict when they will manifest into actual crimes ("risk terrain modeling").[22] With individuals, algorithms have become increasingly better at reconstructing the "modus operandi" of criminals as well as identifying the behavior of criminal organizations.[23] Some cities, such as Kansas City and Chicago, even use programs to create lists of individuals who are most likely to commit a crime.[24] New Orleans recently partnered with Palantir to develop technology that identified the 3,000 people most likely to engage in gun violence.[25]

Ultimately, in a range of forms and sophistication, predictive policing tactics are being adopted by police departments across the country.[26] This wide-scale evolution and innovation within policing, however, also comes with an array of challenges. Accordingly, legal scholars and policymakers have identified a common set of major issues across predictive programs.

First, as with many significant innovations in law enforcement, predictive policing leads to concerns about transparency and

U. PA. L. REV. 327, 363-64 (2015) [hereinafter Ferguson, *Big Data*] ("Finally, because commercial entities — rather than the government — own these 'fourth party' records, they avoid many of the constitutional and statutory protections that might ensure privacy of these records.").

[21] *See* PERRY ET AL., *supra* note 13, at 19-55.

[22] *See* Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 277-84 (2012) [hereinafter Ferguson, *Predictive Policing and Reasonable Suspicion*]; *see also* PERRY ET AL., *supra* note 13, at 50-51, 55.

[23] *See* Ferguson, *Big Data*, *supra* note 20, at 371.

[24] *See* Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 956 & n.36.

[25] *See* Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1113, 1146 (2017) [hereinafter Ferguson, *Policing Predictive Policing*].

[26] *See, e.g.*, PERRY ET AL., *supra* note 13, at 64-76; Simmons, *supra* note 24, at 954-57. *See generally* Ferguson, *Policing Predictive Policing*, *supra* note 25, at 1115-16 ("Major cities in California, South Carolina, Washington, Tennessee, Florida, Pennsylvania, and New York, among others, have purchased new predictive policing software to combat property crimes such as burglaries, car thefts, and thefts from automobiles.").

oversight.[27] In certain regards, transparency can be seen as a check on government. As police departments retain growing amounts of personal information and increasingly rely on tactics shaped around analysis of such data, transparency helps encourage a certain level of accountability and quality to the process.[28] Additionally, transparency also creates opportunities for private sector involvement, facilitating input on improving practices or software.

In general, proposals regarding public disclosure vary in reach, but largely emphasize the importance of (a) notice to individuals impacted by programs, (b) robust internal audit procedures, and (c) the opportunity for communities to be meaningfully heard, once informed of the scope of the automated program. But in order for disclosures to mean anything in practice, people need to be able to understand how this software actually works. An initial barrier here, discussed below, is the fact that private companies are reluctant to offer up their proprietary algorithms for the world (and competitors) to see.[29] But even if courts or oversight bodies had access to a product's source code or algorithmic assumptions, someone needs to be able to explain what they all mean.[30] Are acceptable factors being considered? How are they being weighed? What metrics should be used to measure their efficacy? All of these open issues demonstrate the innate hurdles to oversight and the limits of transparency as a good in itself.

Second, there is a possible tension between the widespread use of predictive programs and civil rights protections. The overall efficacy of this technology is a debated question.[31] Yet, aside from the discussion of predictive policing's possible benefits, some have raised concerns that the manner "police are adopting and using these technologies means more people of color are arrested, jailed, or physically harmed

[27] For an instructive discussion of transparency and oversight in the context of courts and police operations, see generally Andrew Manuel Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. 2049 (2016).

[28] *See* Zarsky, *supra* note 7, at 1533-41 ("The most basic and popular justification for transparency is that it facilitates a check on governmental actions.").

[29] *See* Simmons, *supra* note 24, at 995.

[30] *See* Rich, *supra* note 17, at 906 ("[O]ften no one will be able to explain to a reviewing court how or why the algorithm made its prediction."); *see also* Zarsky, *supra* note 7, at 1526-30. The difficulty of this task is only compounded when machine learning is involved and the underlying product is rapidly evolving on its own accord.

[31] *See, e.g.*, Ferguson, *Policing Predictive Policing*, *supra* note 25, at 1163-64 ("Because the efficacy of the technology remains unknown, jurisdictions seeking to purchase the technology need to check the methodology and prepare responses to future legal and community challenges."); Simmons, *supra* note 24, at 953-57.

by police, while the needs of communities being policed are ignored."[32] To that point, scholars are split as to whether predictive analytics provide objective outputs that can mitigate potential bias,[33] or whether they run the risk of exacerbating existing problems. The latter camp identifies two potential entry points for bias within predictive programs: (a) the direct or indirect use of certain "forbidden factors" (e.g., race) within the algorithms themselves, or (b) the manner that certain "preexisting biases" present in the underlying data are compounded once employed by the algorithm.[34]

Third, many have raised privacy concerns regarding both the collection of personal data and its use in justifying interventions. As law enforcement collects more individual pieces of information — each perhaps innocuous standing on its own — agencies are able to gradually construct a rather complete, intimate profile of an individual.[35] Simply maintaining these databases inherently prompts questions about how current Fourth, Fifth, and Sixth Amendment doctrines apply to new, previously unconsidered technological frontiers.[36]

Additionally, big data programs materially expand the information available to police officers when they are making determinations about the reasonableness of a stop, search, or arrest.[37] Imagine a situation where officers see an individual engaged in "furtive" movements — perhaps pacing around a storefront or unoccupied home — and they

[32] Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 49 GA. L. REV. (forthcoming 2017) (manuscript at 5). *But see* David Weisburd, *Does Hot Spots Policing Inevitably Lead to Unfair and Abusive Police Practices, or Can We Maximize Both Fairness and Effectiveness in the New Proactive Policing?*, 2016 U. CHI. LEGAL F. 661, 665 ("[T]he evidence base for hot spots policing is very strong. But in recent years, like other new proactive policing strategies, it has come under attack because of concerns that it leads to biased and abusive policing practices.").

[33] *See, e.g.*, PERRY ET AL., *supra* note 13, at 1 ("Forecasting is considered objective, scientific, reproducible, and free from individual bias and error.").

[34] *See* Simmons, *supra* note 24, at 970-83.

[35] *See* Joh, *supra* note 15, at 60; *see also* Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105, 107 (2014) (noting a "triple threat" to privacy that "stems from total surveillance, big data analytics, and actuarial trends in policing").

[36] *See generally* Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 826-36 (2010).

[37] Two data-expanding developments in policing have gained particular attention recently: body cameras and facial recognition software. For a discussion of these topics, respectively, see, for instance, *Developments in the Law — Policing: Chapter Four: Considering Police Body Cameras*, 128 HARV. L. REV. 1794 (2015); Mary D. Fan, *Justice Visualized: Courts and the Body Camera Revolution*, 50 UC DAVIS L. REV. 897 (2017).

are faced with the decision to stop and search the possibly suspicious person. Depending on the program at hand, they may discover the individual is on a local "heat list"[38] or that the neighborhood is deemed at risk for robberies.[39] How, and to what extent, can officers use this information?[40] Are we punishing specific persons for their general communities?[41] Is current Fourth Amendment doctrine even capable of balancing individual privacy rights with this revolution in policing? Alternatively, when can such information make policing decisions *better*, perhaps lending objectivity to otherwise subjective considerations?

These major themes intersect with a number of policy decisions that come with the adoption of predictive policing techniques. And as we will see later on, navigating these tradeoffs reveals key insights applicable outside of the policing context.

B. Predictive Analytics in Health Care

The use of predictive analytics in health care is burgeoning. For instance, physicians already use this technology in the context of prognostic models. Predictive analytics help doctors utilize data from Electronic Health Records, harnessing "thousands of rich predictor variables," to produce likely better models than currently available ones such as the Acute Physiology and Chronic Health Evaluation ("APACHE") score and the Sequential Organ Failure Assessment ("SOFA") score, which are currently limited to "only a handful of variables, because humans must enter and tally the scores."[42] Looking ahead, consider how improvements in computer vision and the ability to compare a particular x-ray to hundreds of thousands that have already been coded, will alter or reduce the role of radiologists. In fact, algorithms can already replace the read of a mammogram by a second radiologist today.[43] Some also have proposed and begun to put in practice uses of predictive analytics to address some of the major drivers of health care costs, such as: high-cost patients, hospital

[38] *See* Ferguson, *Policing Predictive Policing*, *supra* note 25, at 1143-46.

[39] *See* Ferguson, *Big Data*, *supra* note 20, at 330.

[40] Indeed, following *Illinois v. Wardlow*, 528 U.S. 119 (2000), whether or not a neighborhood is a "high crime area" is already a significant — often dispositive — factor in the Fourth Amendment analysis.

[41] For an interesting take on this question, see generally Crespo, *supra* note 27, at 2078-82.

[42] Ziad Obermeyer & Ezekiel J. Emanuel, *Predicting the Future — Big Data, Machine Learning, and Clinical Medicine*, 375 NEW ENG. J. MED. 1216, 1218 (2016).

[43] *Id.*

readmissions, and optimizing treatment for diseases that affect multiple organ systems.[44] In a more sinister vein, some too have alleged that health "insurers use data-mined prescription drug data to continue their discrimination against high-cost patients by moving drugs associated with patients with expensive chronic conditions to high cost-sharing tiers in the hope of discouraging those patients from applying for coverage."[45] There are many other examples.

The legal literature on predictive analytics in health care is at this moment less robust than that on predictive policing, although that is changing.[46] Here are some of the key questions being debated in this literature, some of which we will discuss in greater depth below: What liability will lie against physicians who rely on black box algorithms or the makers of the software when patients experience adverse events they allege are related to the algorithm, and how will courts frame the relevant duty of care?[47] Who owns patient records such as electronic health records, in what circumstances can they be data mined, and does that require explicit consent?[48] How should Human Subjects Research regulations apply to big data research?[49] How does the Health Insurance Portability and Accountability Act (better known as "HIPAA") apply to health care big data and how might it be altered to deal with the unique privacy issues raised by big data?[50] How should

[44] David W. Bates et al., *Big Data in Health Care: Using Analytics to Identify and Manage High-Risk and High-Cost Patients*, 33 HEALTH AFF. 1123, 1124 (2014).

[45] Nicolas P. Terry, *Big Data and Regulatory Arbitrage in Healthcare*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 90).

[46] At the risk of some horn tooting, one of us just edited a new book on this subject: BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9.

[47] *E.g.*, W. Nicholson Price II, *Medical Malpractice and Black-Box Medicine*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 410-24) [hereinafter Price, *Medical Malpractice*]; *see, e.g.*, Cohen et al., *Legal and Ethical Concerns*, *supra* note 4.

[48] *E.g.*, I. Glenn Cohen, *Is There a Duty to Share Health Care Data?*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 293-312) [hereinafter Cohen, *Duty to Share*]; *see, e.g.*, Jennifer Kulynych & Henry T. Greely, *Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights with Research When Privacy and Science Collide*, 4 J.L. & BIOSCIENCES 94 (2017).

[49] *E.g.*, Liza Dawson, *The Common Rule and Research with Data, Big and Small*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 332); Laura Odwazny, *Societal Lapses in Protecting Individual Privacy, the Common Rule, and Big Data Health Research*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 317); Kulynych & Greely, *supra* note 48, at 113-15.

[50] *E.g.*, Margaret Foster Riley, *Big Data, HIPAA, and the Common Rule: Time for Big Change?*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 351-52). *See generally* Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143 (2017) (discussing how to

the need for transparency and validation of predictive analytic algorithms be balanced against the needs for trade secrecy or other intellectual property protections?[51] How can the Food and Drug Administration ("FDA") best evaluate the use of predictive analytics in products such as clinical decision support?[52] There are many more such questions of legal interest out there, and still more yet to be encountered, but this gives a good introduction to the relevant literature.

II. WHAT CAN THE DOC AND COP TEACH EACH OTHER?

Given that the legal literature on predictive policing is now fairly well developed while the equivalent literature on predictive analytics in health care is in a more developmental stage, in this Part we engage in an exercise in arbitrage: What can the legal thinking on the policing side enrich in the legal thinking in the health care side and vice versa? We arrive at some answers by comparing the two subject matters. To be clear at the outset, we believe that this exercise can be valuable regardless of how someone comes down on the various normative questions within each field. To put the point otherwise, both critics and champions of the use of predictive analytics in one domain may have something valuable to learn by thinking about the other domain.

A. *Big Data and Equality*

The use of predictive analytics in both policing and in health care raises the specter that discrete and insular minorities may be particularly disadvantaged by the system.

To date, these concerns have been voiced much more explicitly in the policing side. As Solon Barocas and Andrew Selbst have put it, there is a real risk that "data mining can reproduce existing patterns of discrimination, inherent in the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society."[53] To be

address privacy issues raised by health care data outside the HIPAA domain).

[51] *E.g.*, Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1142; W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419, 443-53 (2015) [hereinafter Price, *Black-Box*].

[52] *E.g.*, Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1145; W. Nicholson Price II, *Regulating Black-Box Medicine*, MICH L. REV. (forthcoming 2018) (manuscript at 22-66) (on file with authors) [hereinafter Cohen et al., *Regulating Black-Box*]; Jeffrey M. Senger & Patrick O'Leary, *Big Data and Human Medical Judgment: Regulating Next Generation Clinical Decision Support*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 393).

[53] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L.

sure, as Selbst concedes, thus far "discrimination has not been directly observed in predictive policing," but he chalks that up to the fact that such assessments "either do not exist or are proprietary."[54] Selbst suggests five steps in the workflow of predictive policing where "disparate impact on protected classes" (though their focus is race) can be mitigated: "designing the problem, collecting the training data and labeling examples within it, selecting features to model, and the potential for accidentally using proxies for protected class."[55] Andrew Ferguson proposes a nine-factor analytical framework for evaluating the implementation of predictive technologies in police departments,[56] intended in part to identify and mitigate the impacts of "racial and class-based bias" within programs.[57]

If the fear for predictive analytics in policing is that it over-includes minorities and leads to too many resources spent on policing such communities, in health care it is exactly the opposite. As Malanga, Loe, Robertson, and Ramos have suggested, the concern is that in health care:

> [B]ig data has not captured certain marginalized demographics. Particularly concerning are racial minorities, people with low socioeconomic status, and immigrants. Many of the people missing from the data that comes from sources such as internet history, social media presence, and credit card use are also missing from other sources of big data, such as electronic health records (EHR) and genomic databases. The factors responsible for these gaps are diverse and include lack of insurance and the inability to access healthcare, to name just two, which leaves those missing from the data at an even greater disadvantage and more susceptible to missing out on the healthcare advantages and benefits that big data can

REV. 671, 674 (2016).

[54] Selbst, *supra* note 32 (manuscript at 12). Their underlying thesis, however, is not universally shared. *See, e.g.*, Weisburd, *supra* note 32, at 686 ("I have argued that hot spots policing properly implemented is likely to lead to less biased policing than traditional strategies. Moreover, there is little evidence that hot spots policing per se leads to abusive policing practices.").

[55] Selbst, *supra* note 32 (manuscript at 19); *see also* Barocas & Selbst, *supra* note 53, at 675-92. For a different take, see Shima Baradaran, *Race, Prediction, and Discretion*, 81 GEO. WASH. L. REV. 157, 163 (2013) (arguing that predictive policing seems to disadvantage white defendants and black victims, not black defendants).

[56] *See* Ferguson, *Policing Predictive Policing*, *supra* note 25, at 1119 (proposing a framework analyzing "data, methodology, social science, transparency, accountability, practical implementation, administration, vision, and security").

[57] *Id.* at 1153-54.

> provide. Further exacerbating the problem is the fact that many of the people who are unable to integrate into the large data trail are the very people most in need of increased health research, intervention, and care.[58]

There are a variety of interventions that might be used to try to counteract these deficits, from mandating increased minority inclusion in clinical trials, to the Precision Medicine Initiative, to utilizing other sources to statistically correct for knowable data gaps.[59] But Malanga et al. candidly concede there is no silver bullet,[60] and in the health care context there is a tension between the desire to de-identify data more thoroughly (for privacy protective reasons) and the ability to assess and implement some of these solutions.

We see opposite forces (over versus under inclusion of minority data) leading to a similar outcome — a perceived failure to treat minorities as well as majority populations. Moreover, in both settings we must never forget to ask the "as against what" question, and consider whether even imperfect use of predictive analytics here may be better than the status quo way minorities are treated currently. Beneath these similarities on equality of data issues is one important difference, though, related to normative evaluation. In the health care space, if predictive analytics serves minority populations in a poorer fashion than the majority, that is an uncontested "loss" — a result tolerated but not desired by anyone involved in the system design. In the policing context, by contrast, the politics are more complicated. There is much sharper political contestation of what the right level of minority policing ought to be.[61] This is in part due to deep-seated

[58] Sarah E. Malanga et al., *Who's Left Out of Big Data? How Big Data Collection, Analysis, and Use Neglects Populations Most in Need of Medical and Public Health Research and Interventions*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS, *supra* note 9 (manuscript at 145).

[59] *Id.* at 155-61.

[60] *Id.* at 162.

[61] *Compare, e.g.*, Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L.J. 2054, 2117 (2017) ("Much of the early critique of police officers' treatment of racially and socioeconomically marginalized neighborhoods (or what many scholars call 'the ghetto') stemmed from law enforcement's neglect of those communities, leading to some mid-twentieth century racial justice advocates to urge police to become more active in poor urban neighborhoods. Yet several forces converged in the 1970s, 1980s, and 1990s that shifted the problem from one of utter neglect to the current problem of overpolicing and underprotection."), *and* Jordan Blair Woods, *Decriminalization, Police Authority, and Routine Traffic Stops*, 62 UCLA L. REV. 672, 745 (2015) (discussing how overpolicing can "jeopardize perceptions of personal security in entire communities," especially in minority communities), *with* Lawrence W. Sherman & David Weisburd, *General Deterrent Effects of Police Patrol in*

disagreements about the merits of broken windows theories of policing and further divisions among various communities about what intensity of resources devoted to policing minority communities is desirable versus counterproductive. These splits are exacerbated by additional gaps between individuals' perceptions of the crime rate and the data-driven reality. In short, what constitutes a "win" and a "loss" — let alone determining the causes of certain outcomes — appears materially more muddled and disputed in the policing context. As a result, we suspect that at the policy level it will be harder to motivate change on this issue in the policing as opposed to the health care realm.[62]

B. Role Disruption, Training Gaps, and Reason Giving

Predictive analytics presents itself as disruptive technology. Both medicine and policing are long-standing, well-organized professions with strong well-established training processes and settled historical traditions about how "things are done." The tension is obvious and manifests itself in each of the settings.

When it comes to health care:

> The role of the physician in the delivery of care across inpatient and outpatient settings may need to be reconfigured. The separation of hospitalists from ambulatory care providers, the frequent handoffs of responsibility for inpatients from one physician to another, and the rarity of long-term primary care relationships all mean that when a predictive analytics model identifies a patient as being at risk, the treating physician might not know the patient or his or her values and preferences.

Crime "Hot Spots": A Randomized, Controlled Trial, 12 JUST. Q. 625, 645 (1995) (finding that police presence increases in certain targeted regions reduces crime and disorder in previously high-crime areas), *and* William J. Bratton et al., *This Works: Crime Prevention and the Future of Broken Windows Policing*, MANHATTAN INSTITUTE (May 1, 2004), https://www.manhattan-institute.org/html/works-crime-prevention-and-future-broken-windows-policing-5629.html ("Broken windows works. Not by itself, but as part of a master set of strategies.").

[62] That said, as one astute reader of this article reminded us, there may also be countervailing reasons to be *more* optimistic about the police context: (1) the data is already available as opposed to having to be collected, and (2) the effect on minority populations is more immediate and easier to measure in the policing rather than the health care context, in part because health effects take more time to manifest in some instances and may be noisier in terms of measurement.

> A model's predictions also raise novel questions about the doctor-patient relationship. Traditionally, a single physician provided care to an individual patient based on the patient's best interests, as guided by his or her preferences and values. In the era of predictive analytics and team-based care, clinical decision making may be heavily influenced by default rules set by the health care organization. These rules may be driven by financial and administrative incentives and by a desire to maximize population-based health. It may seem to patients that the treating physician is no longer exercising clinical judgment and acting in their best interests.[63]

The extent of the disruption of the physician's role depends in large part on how much discretion is afforded to the physician and how easily such discretion can be exercised under the choice architecture of implementation for predictive analytics in a particular setting. This raises a corollary concern: Is the current state of medical education adequate to make physicians (as well as nurses, hospital administrators, etc.) wise users of predictive analytics? Medical education is already densely packed with a myriad of kinds of learning, but data science has traditionally not been a focus. Would widespread adoption of predictive analytics be met with widespread improvements in data science education in medical school, or would (and should?) it become a specialized set of learning for a subset of physicians with others just told to "trust the algorithm"?[64]

Machine learning algorithms, though, raise a special set of disruptive concerns especially because of the fiduciary nature of the physician-patient relationship. Imagine a woman undergoing treatment for breast cancer and trying to decide whether to opt for partial or the much more invasive radical mastectomy. The doctor recommends the radical mastectomy. When asked why, he says "for

[63] Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1146-47.

[64] Lest that be thought of as pejorative, such rational ignorance is the norm not only for medicine but for most professions. The average physician could not explain exactly how an MRI works, nor could the average law professor (or student) explain exactly how the word processor he types this Essay on does. A quite different concern about increased use of predictive analytics in health care is whether it will contribute to the very real issue of physician burn-out. Recently Medscape estimates found that physicians reported the computerization of practice and Electronic Health Records as one of the leading causes of burnout. Carol Peckham, *Medscape Lifestyle Report 2017: Race and Ethnicity, Bias and Burnout*, MEDSCAPE (Jan. 11, 2017), https://www.medscape.com/features/slideshow/lifestyle/2017/overview#page=4. Of course, it is possible that predictive analytics, if implemented well, may also help to *reduce* burn out.

patients like you we know from the data that it tends to be the best option." When she asks "what is it about my case that makes you think that," shall he respond "the algorithm has examined 10,000 variables from your EHR and, based on its validated model, determines this is what is appropriate in your case"? To be sure that may be much *better* than answering as the current physician might that "given the limited number of patients I have seen in my practice, what I learned in medical school, and what I have read in the literature, I think this will be better for you" — but will the patient accept the former answer as better? Does the medical fiduciary relationship have a requirement of reason giving that is in tension with machine learning? After all, in machine learning the reasons why an answer is arrived at can often not be provided.[65]

Somewhat similar concerns are present, though perhaps in somewhat more muted forms, in predictive policing. As Ferguson puts it well:

> [W]ithout significant investment in exposing the data collection methods, weaknesses, and gaps, and without equal investment in understanding the challenges associated with inputting and analyzing the data, the entire system runs the risk of being built on an unknown and unknowable database. The nature of algorithms further obscures the process, except perhaps to technical experts. Police officers and administrators receive the results, but due to the complexity of the chosen algorithm they can rarely understand the underlying math. Thus, predictive policing runs into the same problems as other

[65] Some might think that machine learning decision-making is in tension with human dignity. In much of the literature there is certainly a whiff of this suggestion, which is in turn not uncommon in discussions of automation's effect elsewhere, such as in the workforce. Some like Tal Zarsky, though, have pushed back on any simple connection between automation and dignity:

> Linking the lack of dignity and automation is, I believe, an anachronistic notion. In the twenty-first century, one need not fear a computerized process. If computerized searches can provide fair and efficient outcomes, should they still be considered as undignified? Indeed, safeguards (through either transparency or other measures) should be applied to all steps which might compromise rights of individuals and seem arbitrary, be they automated or manual. The level of automation needs not, on its own, merit a higher level of transparency.

Zarsky, *supra* note 7, at 1552. We tend to agree that there is no necessary dignitarian harm in automation, but in some circumstances claims of dignitarian harm from lack of *reason giving* due to automation seem more plausible.

> automated predictive technologies: the technical complexity of the design makes it nearly impossible for outsiders to determine the accuracy, effectiveness, or fairness of the program. True, police can see if the system works, but police cannot see how the system works. This lack of transparency is not simply the result of new technology, but also the influence of the proprietary nature of the software.[66]

The reason the concerns are more muted, which we discuss in greater depth below, has to do with the relationship of those who employ the predictive analytics and those who are benefited and harmed by it in the two contexts. Both patients and citizens are owed reason-giving for the choices that are made, but concepts like informed consent in the medical context, patient-physician confidentiality, and the spirit of the Hippocratic Oath create a much more one-to-one relationship of reason giving. As a patient, I have the right to ask my doctor to explain how important decisions are being made about my health. As a citizen, my right to demand information explaining how important policing decisions are made is much more diffuse,[67] and relies much more heavily on the political process than a fiduciary one-to-one relationship.[68] Moreover, as discussed below, there are in some circumstances justified grounds for secrecy to do with policing techniques just as there are with "small data" investigatory strategies. That said there are certainly commonalities, and some have made more domain general critiques of this tendency.[69]

[66] Ferguson, *Policing Predictive Policing*, *supra* note 25, at 1170.

[67] To be clear, this is true when we think about policing through the lens of a police department — policed community macro relationship. But it begins to fray when individualized to the officer-suspect level. At that point, the Fourth Amendment largely requires particular reason-giving by officers seeking to stop, frisk, or arrest someone. This dynamic is partially substantiated by later adversarial processes, such as litigation concerning suppression motions or civil rights lawsuits under Section 1983.

[68] *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1831 (2015) ("Policing agencies may not be entirely immune from democratic oversight — police chiefs typically serve at the pleasure of the mayor, police commission, or city council, and sheriffs are directly elected by the people."). *But see* Crespo, *supra* note 27, at 2062 ("Genuine democratic authorization . . . is often hard to attain in the poor, urban, minority communities that live on the criminal justice system's front lines.").

[69] *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 7 (2014) ("Just as automated killing machines violate basic legal norms, stigmatizing scoring systems at the least should be viewed with caution. We should not simply accept their predictions without understanding how they came about, and assuring that some human reviewer can

As with health care, it is unlikely that many police officers (not only in rank and file but even high up in supervisory positions) will have the data science training necessary to understand the basis for which predictive analytics algorithms work in policing. It is hard to know, normatively speaking, what to make of this reality. On the one hand, few officers understand the way in which DNA testing works either, but that does not stop them from being effective users of the information that such testing generates. At the same time, some have worried about function creep having bad consequences in the DNA context. Erin Murphy, for example, has expressed concerns that the availability of the technology in using partial DNA matches has led police to use their resources in a way that is unproductive even from a purely investigatory standpoint.[70] Similar concerns have been raised about how officers may use predictive policing tools.[71] The bigger worry, it seems to us, is not so much as to who understands *how* predictive analytics works but who understands *whether* (and to what extent) it works.[72]

respond to serious concerns about their fairness or accuracy. Scoring systems are often assessed from an engineering perspective, as a calculative risk management technology making tough but ultimately technical rankings of populations as a whole.").

[70] Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 317-18 (2010).

[71] *E.g.*, Ferguson, *Policing Predictive Policing*, *supra* note 25, at 1183 ("In the predictive policing context, this focus might result in following the judgment of algorithms at the expense of other information. In the Predictive Policing 1.0 context, this could just amount to a waste of resources (such as sending patrol cars to the wrong box). But in the Predictive Policing 3.0 context, it could lead to erroneous contact with individuals wrongfully suspected of a crime.").

[72] Ferguson has suggested that such evaluations have not been rigorous in this setting:

> Simply put, for Predictive Policing 1.0 and 2.0, there have been no sustained studies demonstrating cause and effect. Crime rates go up and down. Even in jurisdictions that have adopted PredPol with initial success, crime rates have later risen for unknown reasons. Thus, as a measure of internal validity, the question is still open as to whether any particular predictive policing technology really shows a causal success.

Id. at 1159; *see also* Crespo, *supra* note 27, at 2104-06 ("Appeals to greater empiricism in the judicial process often encounter a common initial hurdle: the potentially limited competency on the part of judges and litigants to compile, organize, and digest sometimes complex empirical information."). *But see generally* Tracey L. Meares, *Three Objections to the Use of Empiricism in Criminal Law and Procedure — and Three Answers*, 2002 U. ILL. L. REV. 851, 851-52 (2002) (arguing for the importance and wider use of empiricism in crafting criminal law and procedure).

C. Complementing v. Supplanting and the Risks of Automation Bias

There is a very real concern in both fields of allowing predictive analytics to put users on autopilot. Much as we often trust Spotify to pick the next song or Waze to map the best way back home, there is an intuitive appeal for both doctors and cops to rely extensively on the judgment of software. As algorithms grow in sophistication, it becomes more difficult to opt instead for personal judgment. A challenge then is distinguishing reflexive reliance from shrewd deference when it comes to employing computerized models.

Predictive analytics is best used to *complement* rather than *supplant* human judgment. But the rush to adopt this technology may lead to several risks inherent to the latter. Accordingly, as discussed below, predictive policing may establish a framework for avoiding these problems in the health care context. There are three main areas of concern inherent to the "imperfect implementation" of predictive analytics in health care.[73]

First, compromised quality. As Ziad Obermeyer and Zeke Emanuel noted:

> [L]etting the data speak for themselves can be problematic. Algorithms might "overfit" predictions to spurious correlations in the data, or multiple collinear, correlated predictors could produce unstable estimates. Either possibility can lead to overly optimistic estimates of the accuracy of a model and exaggerated claims about real-world performance. These concerns are serious and must be addressed by testing models on truly independent validation data sets, from different populations or periods that played no role in model development. In this way, problems in the model-fitting stage, whatever their cause, will show up as poor performance in the validation stage. This principle is so important that in many data-science competitions, validation data are released only after teams upload their final algorithms built on another publicly available data set.
>
> Another key issue is the quantity and quality of input data. Machine learning algorithms are highly data hungry, often requiring millions of observations to reach acceptable performance levels. In addition, biases in data collection can substantially affect both performance and generalizability. Lactate might be a good predictor of the risk of death, for

[73] *See* Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1146.

> example, but only a small, nonrepresentative sample of patients have their lactate levels checked. Private companies spend enormous resources to amass high-quality, unbiased data to feed their algorithms, and existing data in electronic health records (EHRs) or claims databases need careful curation and processing to become usable.[74]

Second, checkered results may materially undermine trust — be it from patients, providers, or other stakeholders. This early impression may stunt their overall adoption.[75] Third, initial difficulties and problematic rollouts may cool the market for such technologies, thereby cribbing innovation within a vitally important set of products.

These concerns map relatively well onto the growth of predictive policing.[76] The perception alone of poor policing can fatally undermine a community's trust in both law enforcement and their chosen policing strategies.[77] Thus departments and policymakers have needed to contemplate both *ex ante* and *ex post* measures to promote the prudent use of predictive analytics.

When it comes to shaping predictive policing *before* the stop or search happens, policymakers and legal scholars have focused on the impact of big data on the Fourth Amendment's "reasonable suspicion" standard. As noted in *Terry v. Ohio*, police officers are tasked with making a reasonable judgment call from the present information. But how does the widely expanded array of information now available to officers impact this test? For instance, can an officer base his decision exclusively on factors derived from computerized models?[78] The

[74] Obermeyer & Emanuel, *supra* note 42, at 1217; *see also, e.g.*, Sendhil Mullainathan & Ziad Obermeyer, *Does Machine Learning Automate Moral Hazard and Error?*, 107 AM. ECON. REV.: PAPERS & PROC. 476, 476 (2017) ("In automation tasks, measuring *y*, e.g., majority opinion of ophthalmologists, is straightforward. In health policy applications, we rely on electronic health records or claims data to measure *y* and *x*. The very construction of these data induces large and systematic mismeasurement. These in turn can bias algorithmic predictions; in some cases, these biases can automate policies that magnify existing clinical errors and moral hazard.").

[75] *See* Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1146.

[76] A wrinkle, as discussed more below, is that the institutional trust relationship between police departments and policed communities is significantly more fragmented, fraught, and complicated due to racial and socioeconomic lines.

[77] *See* Weisburd, *supra* note 32, at 673-74; *see also* Friedman & Ponomarenko, *supra* note 68, at 1854 (noting the political consequences of public "discontent" over stop, question, and frisk in New York City).

[78] Ferguson posits a hypothetical where a robbery suspect is deduced exclusively by predictive policing tactics and poses this question as "whether a Fourth Amendment stop can be predicated on the aggregation of specific and individualized, but otherwise noncriminal, factors." Ferguson, *Big Data*, *supra* note 20, at 330.

general current consensus is no, with some analogizing predictive analytics to current tools like drug-sniffing dogs or police informants.[79] Thus, departments need to ensure that officers still look to a totality of the circumstances when making a decision, using big data as a factor but not a dispositive one.[80] But *after* the intervention, how do we know its precipitating calculation was acceptable? This inquiry intersects a good deal with the discussion of transparency below,[81] and underscores the need for some sort of external evaluative framework for law enforcement tactics.[82]

The implementation of predictive policing therefore provides three general guideposts for doctors in this space. First, practitioners need to understand not only what these products do, but more importantly what they *do not* do.[83] Second, health care providers should structurally borrow from the conceptual role (how it plays out in actuality is another matter) that the Fourth Amendment factors in predictive policing, developing certain *ex ante* standards to manage how individual practitioners approach information derived from predictive analytics. Some of this will relate to the more general points about training in data science discussed above, but much of this will also be health system or even device specific. One interesting set of questions is what, if any, role medical malpractice has to play in this issue, a topic discussed below. And third, hospitals and similar organizations should develop a robust *ex post* framework of oversight,

[79] *E.g.*, Rich, *supra* note 17, at 902.

[80] *See* Ferguson, *Big Data*, *supra* note 20, at 349 ("Thus, knowledge about the suspect cannot alone justify a stop; the officer's knowledge must be tied to a suspected criminal activity, past or present.").

[81] *See supra* Part I.A for a discussion of transparency.

[82] Erin Murphy offers a good example of an effective framework by sketching the contours of a constitutional criminal procedure for databases around five key characteristics. For instance, Murphy argues that databases "require structural, rather than individual, oversight." Murphy, *supra* note 36, at 826; *see also* Crespo, *supra* note 27, at 2070-101 (describing a system for how big data can be used to support external checks over police probable-cause analyses, namely through informed judicial assessments of their consistency, descriptive accuracy, and predictive accuracy).

[83] RAND identifies one of the major "myths" of predictive policing as "the computer will do everything for you." *See* PERRY ET AL., *supra* note 13, at 117-18. Furthermore, Joh describes two of the pitfalls that can accompany excessive deference to the models: "First, no predictive policing program is entirely objective . . . . Second, prediction models might nudge police judgments in favor of investigative detention in borderline cases because the police rely too heavily on probabilistic information." Joh, *supra* note 15, at 58-59. These considerations underscore how it is equally important for departments to both understand whether certain software works and also be able to communicate its particular limitations to on-the-ground officers.

reviewing both the implementation of computerized models as well as the efficacy of the models themselves.

This approach, perhaps revealingly, largely avoids any normative conclusion on the substantive merits of discretion in either field; rather, it treats human judgment as an inevitable, necessary feature of both jobs. There is a creeping question in the background as to whether predictive analytics will eventually evolve to a point where it is objectively desirable to have the computers subsume more and more judgment calls, similar maybe to the point where self-driving cars become the rational (although not perfect) option over human driving. Ancillary to this discussion, too, are questions of what it would take to get to this point. For instance, would police departments need to aggregate an unacceptable amount of personal information in order to eventually create predictive models that have a superior sense of judgment? More on that below.

The foreseeable future, in both policing and health care, nonetheless calls for an informed balance concerning how large a role to allow for independent human discretion. Calibrating that balance will admittedly be very hard. If one errs on too much human review, some of the benefits of implementing these systems — speed, savings on labor, lower error rates, and the like — are likely lost. If one errs towards too little human "second-guessing," the potential overall error frequency reduction (a big uncertainty) may be offset by an erosion of the trust of the system users, which is essential to good results in both policing and in health care. But, to complicate matters further, the level of trust in the system is not exogenous to how often and how deeply such predictive analytic systems are implemented. We now are extremely trusting (perhaps too trusting?) of e-commerce and ATMs in a way that would be unthinkable to someone living in our parents' (or depending on the age of your grandparents') generation. In a chicken-and-egg sort of way, if predictive analytics engines become equally ubiquitous, the delicate balance would look quite different.

D. Liability

One important difference between health care and policing is the standard of liability for practitioners and the effects it has on use of predictive analytics. In health care, liability may lie against the provider who uses predictive analytics, his or her hospital system, the producer of the device or software employing the analytics, or potentially all of the above.[84] To be sure this is an area with precious

[84] Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1144.

little case law, but as against the provider, there are multiple theories of liability. Case law on electronic health records suggests that "physicians can be held liable for harm that could have been averted had they more carefully studied their patients' medical records."[85] The pairing of analytics with decision support raises some particularly thorny issues. For instance, while it is "clinically appropriate to override many computerized alerts in the practice of medicine," there "is a significant risk that 'a doctor who is accustomed to overriding alerts may become desensitized to them and occasionally ignore a critical one,' and evidence of a doctor's overriding alerts may prove damaging in litigation."[86] Indeed physicians may find themselves in a bit of a damned-if-you-do-damned-if-you-don't situation, in that courts may conclude that a "trained provider should be subject to the exact same standard of negligence irrespective of whether clinical decision support software is used, because any treatment decisions are ultimately her own."[87] As Nicholson Price explains:

> Providers could [] be held liable for harmful use of black-box medical algorithms, depending on the prevailing customary practice, and the extent that custom is considered dispositive. As with medical innovation more generally, there is a risk of liability during this transition phase, which presents an opportunity to consider how tort law might encourage the most beneficial medical practices.[88]

The concern is that this liability may chill the adoption of predictive analytics in health care, though some of the descriptive work on jury behavior for decision aids suggests that juries are less likely to find liable physicians who follow such tools.[89]

Beyond the provider, there are other targets of liability. Without going too deep into the weeds, some hospitals may not only face vicarious liability for the acts of health care providers who are deemed the hospital's agents but also have a direct duty to "provide adequate facilities for patient care, including well-functioning equipment

[85] Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKELEY TECH. L.J. 1523, 1541 (2009).

[86] Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1144 (quoting Hoffman & Podgurski, *supra* note 85, at 1547-48).

[87] Price, *Medical Malpractice*, *supra* note 47, at 415-16.

[88] *Id.* at 415.

[89] *Id.* at 418 (citing Hal R. Arks et al., *The Influence of a Physician's Use of a Diagnostic Decision Aid on the Malpractice Verdicts of Mock Jurors*, 28 MED. DECISION MAKING 201, 204-05 (2008)).

necessary for adequate care," or "coordinate care and sometimes a non-delegable duty to actually provide care for patients."[90] Predictive analytics systems could be analogized to other kinds of "equipment" employed by hospitals to attend to patient care, though the analogy frays at the edges. Price has suggested that under this theory:

> [H]ospitals might reasonably be held liable for failing to ensure that the algorithms it makes available to providers and patients are, as a whole, high-quality and safe. Because substantive validation may be impossible in many cases — given the opaque nature of black-box medicine — procedural validation could be required instead. Parallels could be drawn to a more familiar responsibility of hospitals: their requirement to adequately credential the physicians who work in them to ensure that patients are seen by high-quality, well-trained doctors. While a hospital cannot ensure that each decision of its doctors is correct, it can ensure that the doctors it brings through its doors are reasonably proficient. Applying a similar duty to black-box medicine would recognize the inherent opacity of the technology while leaving some responsibility on hospitals to take care in selection and implementation.[91]

If the basic theory of tort law is to be believed, these doctrines — to some contested extent — have both a deterrence effect pushing providers and hospitals to be more careful about their review, selection, and implementation of predictive analytics systems as well as providing compensation to aggrieved patients.

In the world of predictive policing there is much less of a role for liability to play. Legal challenges to overall police practices are rare,[92] and, even when they occur, often do not engage with the technical elements of policing strategies. Take the recent decision in *Floyd v.*

[90] Price, *Medical Malpractice*, *supra* note 47, at 420 (citing Washington v. Wash. Hosp. Ctr., 579 A.2d 177 (D.C. 1990); Thompson v. Nason Hosp., 591 A.2d 703 (Penn. 1991)).

[91] Price, *Medical Malpractice*, *supra* note 47, at 420-21. Predictive analytics software and device designers might also face some liability, but there is a complex set of doctrines in tort law that interpose themselves against recovery. These include the learned intermediary doctrine, which limits drug and device manufacturer liability when a doctor prescribes the item to patients, the immunity of software manufacturers to product liability lawsuits, the possibility of preemption due to approval by the FDA, and difficulties in showing causation. *See* Price, *Medical Malpractice and Black-Box Medicine*, *supra* note 9 (manuscript at 414 n.15) (and sources cited therein).

[92] A major reason for this, naturally, is the doctrine of qualified immunity. *See, e.g.*, Messerschmidt v. Millender, 565 U.S. 535 (2012).

City of New York,[93] where a federal district court judge determined that certain elements of New York City's stop, question, and frisk program violated the Fourth Amendment and Equal Protection Clause of the Fourteenth Amendment.[94] Merits of the decision aside, it is important to note, for predictive analytics oversight purposes, that *Floyd* "did not directly focus on the choice of police tactics, but on the racially disparate impact of the practices."[95] Thus the role of liability within predictive policing is likely smaller than health care because (a) lawsuits are fundamentally more rare, and (b) when they do occur, will probably focus on the potential outgrowths of police strategies rather than the features of the actually technologies used.[96]

E. The Role of Scarcity and the Inevitability of Distributive Choices

In both policing and in health care, predictive analytics as an innovation often (though not invariably) reflects a response to scarcity. Police departments are trying to stretch resources like the number of officers and their hours to most effectively reduce crime and improve communities' sense of safety.[97] Some of the most desirable uses of predictive analytics in health care are aimed at financial cost reduction. On the positive side this can be aligned with patient's own interest such as reducing hospital re-admission rates and optimizing treatment for diseases that affect multiple organ systems.[98] On the more negative side the cost saving elements can sometimes

[93] 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

[94] *Id.* at 667; *see also* Selbst, *supra* note 32, at 36-37.

[95] Ferguson, *Policing Predictive Policing*, *supra* note 25, at 1174; *see also* Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159, 162 (2015) (arguing that stop-and-frisk should be understood programmatically and that stops "are not individual incidents that grow organically" but rather "imposed from the top down").

[96] Future litigation may tend to focus on the underlying technology, however, where there is a close nexus between the software used and the specific legal decision made, such as when judges determine bail or sentencing. For instance, in *State v. Loomis*, 881 N.W.2d 749, 752, 760-61, 766-68 (Wis. 2016), the technology was at the center of the case and the Wisconsin Supreme Court held that a lower court's use of an algorithmic assessment in sentencing did not violate the defendant's due process rights, despite the fact its source code and methodology were withheld from the defense.

[97] *See generally* PERRY ET AL., *supra* note 13, at 118 ("Most police departments do not need the most expensive software packages or computers to launch a predictive program. While there tends to be a correlation between the complexity of a model and its predictive power, increases in predictive power have tended to show diminishing returns . . . .").

[98] Bates et al., *supra* note 44, at 1124.

work to the detriment of patients — for example the allegation that insurers use analytics to determine how to adjust cost-sharing rules for expensive chronic patients with the goal of discouraging them from applying for coverage.[99] The most interesting cases, though, are ones where both effects are present; that is, the use of predictive analytics disadvantages particular patients while advantaging others and overall improves the health for a patient population. For example:

> Imagine a physician who is trying to decide whether to send a patient with moderate organ dysfunction to the intensive care unit (ICU). The patient might benefit from a stay in the ICU, but other patients might benefit more, and ICU beds are limited. An evaluation of the first patient's risk for cardiopulmonary arrest or other preventable serious adverse events might take hours and have limited prognostic accuracy, discrimination, and interrater reliability (or agreement among evaluators). Now imagine that there is a technology [i.e., a predictive analytics program] that could ascertain the risk accurately for a thousand separate patients and continuously update that evaluation every second to help a physician decide whom to send to the ICU.[100]

There are particular patients who, under the pre-analytics world, would have received ICU admission. Some of them would have benefited, some of them would have neither benefited nor been harmed, and potentially (due to nosocomial infections) some might have been harmed. A different set of patients are admitted in a world where the analytics help guide the decision-making and they too may benefit, neither benefit nor be harmed, or be harmed. If the predictive analytics approach is to be used and be justified it must be because *overall* more patients benefit than under the status quo.

That "overall" has a lot bundled into it. It seems to *sub silentio* presuppose a normative criterion of Kaldor-Hicks — the gains to the winners are larger than the losses to the losers such that in theory the winners could compensate the losers and still remain ahead, whether in fact they do — but *not* Pareto superiority for the new distribution, which would require that no one be made worse off. The "overall" also raises a series of subtler distributive questions. These include: In determining that the new distribution is "overall" better, are we willing to aggregate many small gains across larger numbers of people?

[99] Terry, *supra* note 45, at 90.

[100] Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1139.

Would we age-weight gains and losses such that both matter more for younger as opposed to older patients? Should it matter whether patients themselves feel less comfortable with the distributional result knowing it was, at least in part, "done by a computer"?[101] Of course, we should remain aware of the aforementioned "as against what" question — the pre-analytics ICU system is also distributional and merely by virtue of being status quo it should not "get a pass" from ethical analysis.

The larger point, though, is that distributional effects and the need to consider them in designing an analytics system are inevitable. Moreover, the distributional effects must not only be evaluated at the design and implementation stage but on an ongoing basis; not only do systems play out differently in the real world than in the simulation, but importantly, affected communities may react to the analytics in question and alter the distribution of benefits and losses. This fact may be easier to see in the policing context — increased deployment of officer time to region A may cause crime to migrate to region B, to simplify greatly.

That said, while the relationship between police conduct and criminal response may be more intuitively accessible in the policing context, the actual distributional tradeoffs are harder to concretely discern. In the ICU system above, some patients become healthy and some remain (or become) sick: the winners or losers of this arrangement are largely apparent.[102] Policing has less visible metrics. Tradeoffs are almost entirely framed against counterfactuals. Suppose region A sees a reduction in home break-ins but region B has its first murder in years. Is this the outcome of strategic choices or independent macro crime patterns? The difficulty in deciphering

[101] There is a robust literature on these kinds of rationing questions. For a starting point summarizing some of that literature, see generally, for example, A.M. Capron, *The Ethics of Rationing Healthcare*, *in* THE OXFORD HANDBOOK OF U.S. HEALTH LAW 892 (I. Glenn Cohen, Allison K. Hoffman & William M. Sage eds., 2017); I. Glenn Cohen, *Rationing Legal Services*, 5 J. LEGAL ANALYSIS 221 (2013).

[102] This feature, though, may not be generalizable to all health care usage of predictive analytics. After all, health care is a textbook example of a credence good — "one whose quality cannot be detected even after it is experienced"; that is, for patients a recovery is no guarantee of good care since the patient's condition could have improved with no care (indeed it could even have improved faster or more). Maxwell J. Mehlman, *Dishonest Medical Mistakes*, 59 VAND. L. REV. 1137, 1139 n.6 (2006). The *locus classicus* for this point, cited by Mehlman, is of course Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941, 951-52 (1963).

cause-and-effect phenomena in policing makes defining tradeoffs harder since the array of options is hard to determine.

What to take away from this theme? First, adoption of a predictive analytics approach to either policing or health care should not be seen as a mere technocratic means-ends kind of enterprise; both the status quo and the post-implementation worlds involve winners and losers and the redistributions of gains and losses is a moral matter that needs to be thought about and decisions on redistribution need to be defended. Because of the centrality of questions of resource allocation and distributive justice in bioethics, this is an area where the health care context may actually have lessons for the policing one.

Second, the questions raised by this insight are not just questions of *what* distributional re-allocations are justified, but *who* gets to decide. While there may be some areas where distributive justice theory clearly approves or prohibits certain design and implementation choices, much more often there will be grey zones where different moral or political theories will not come to agreement. Who should decide? All citizens? Their representatives? Deliberative democracy fora? Those who will suffer the most? Again, there has been considerable thinking about this in the health care setting, be it patient governance models for biospecimen banks or Norman Daniels' system of Accountability for Reasonableness approach.[103] Some of these may be useful for predictive policing.[104]

But underlying all this analysis is an assumption that such distributional choices are visible to system designers. The fear is that the opacity of the algorithm may cloak the very distributional choices embedded therein. It likely matters what is the cause of the opacity — corporate self-protection, the specialization needed to write and read code, or "opacity that stems from the mismatch between mathematical optimization in high-dimensionality characteristic of machine learning and the demands of human scale reasoning and styles of semantic interpretation."[105]

[103] NORMAN DANIELS, JUST HEALTH: MEETING HEALTH NEEDS FAIRLY 274-96 (2007) (setting out a system for health care rationing by the state that requires that rationales for making decisions must be publicly accessible, that the rationales must be relevant and evidence based, that a mechanism exists for appealing decisions and their rationales, and that there is a compliance system to make sure the preceding conditions are met); *see, e.g.*, Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1142.

[104] These questions as to system-design and decision-making inform the political accountability framework touched on *infra* Part II.G (discussing the benefits, mechanisms, and limitations to transparency within policing).

[105] Burrell, *supra* note 8, at 1-2.

F. The Nature of the Privacy Threat

Although predictive analytics in policing and medicine both involve tremendous amounts of information, the nature of the individual data points is qualitatively different. As a result, concerns about privacy take distinct flavors. Within health care, patients are rightly concerned about the use of their own data. But it is the connection of a data point — for example, a crippling condition — with information about the person that is the main concern for individuals. The essential privacy protections are thus those that prevent the connecting of a patient's identity to his or her medical information when that information is made available (with some de-identification techniques applied) to model developers. HIPAA offers certain methods of acceptable de-identification,[106] but these protections are not ironclad.[107] Beyond malicious attempts to re-identify individual patients, network security and data breaches pose another danger to maintaining patient privacy.[108]

Overall, within health care-based predictive analytics, the system works when people remain anonymous. Personal information is revealed when something goes *wrong*. In a number of ways, the opposite is true for policing. Predictive models strive to produce actionable, concrete outputs for police officers. Consider Chicago's "heat list," referenced herein, which directs cops to keep an eye on "those identified by a risk analysis as most likely to be involved in future violence."[109] In this regard, a person's privacy — especially if understood in the Brandeis and Warren mold of a "right to be let alone"[110] — is compromised when something goes *right*.[111]

[106] Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1141.

[107] *See, e.g.*, Melissa Gymrek et al., *Identifying Personal Genomes by Surname Inference*, 339 SCIENCE 321 (2013) (describing the re-identification of people from genomic sequence data).

[108] *See, e.g.*, Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1141 (health care context); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716 (2010) (more generally).

[109] Joh, *supra* note 15, at 35. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

[110] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[111] It is important to note, however, that not all forms of predictive policing incur the same privacy costs. Jane Bambauer categorizes the sorts of investigations conducted by police, differentiating "crime-out" tactics steeped in predictive analytics from more traditional suspect-first policing. Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 208 (2015) ("Rather than selecting a suspect first and looking for evidence second, crime-out investigations reverse the order."). There is also a strong

This application of predictive policing further muddles the traditional tradeoff debate between privacy and security.[112] As a response, in part, there is a growing focus today on "quantitative" privacy rights prompted by the "advent of gigantic databases filled with personal, behavioral, and biometric data."[113] Unlike health care, individual pieces of data — a general locational point here or a piece of cellphone metadata there — do not themselves usually represent a serious infringement on a person's privacy. But the aggregate of these various data points become parts of a "mosaic" that forms a rather intimate profile of an individual.[114] In a sense, effective predictive policing revolves around turning strangers into known entities,[115] while the use of predictive analytics in health care does not require, and in fact likely discourages, such a getting-to-know-you process.

These dissimilarities in the nature of the information collected and the manner that it is utilized, however, seem to converge around common themes of consent. In both fields, there is a trade-off between systemic and individual interests: individuals likely receive an overall, systemic benefit — be it better health services or more effective policing — when their data is used for predictive analytics but may be unhappy about a lack of individual autonomy in authorizing the data

argument that in certain contexts, surveillance (and related measures) is privacy *enhancing*; that is, we often must determine the *sort* of privacy we value, perhaps favoring government intrusion to curb that of nefarious third parties. *See generally* BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES — CONFRONTING A NEW AGE OF THREAT (2015) (discussing these issues). But this debate is beyond the scope of our project here.

[112] *See, e.g.*, United States v. Jones, 565 U.S. 400, 417-18 (2012) (Sotomayor, J., concurring) ("Perhaps, as Justice ALITO notes, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable' . . . and perhaps not."); *see also* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

[113] Miller, *supra* note 35, at 135-36.

[114] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation."). Christopher Slobogin describes this "mosaic theory" as "the idea that certain types of governmental investigation enable accumulation of so many individual bits about a person's life that the resulting personality picture is worthy of constitutional protection." Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 1, 3-4 (2012).

[115] *See* Ferguson, *Big Data*, *supra* note 20, at 335 ("The wrinkle of big data is that now officers are no longer dealing with 'strangers.'").

use. In health care the question of individual consent for use of Electronic Health Record ("EHR") data is being debated.[116] The matter is more societally hashed-out in policing. For the bulk of the information utilized by police departments, consent is not necessary: data is either "public," compiled under the third-party doctrine discussed above, or collected once an individual establishes probable cause or reasonable suspicion. For a combination of doctrinal and pragmatic reasons,[117] courts and communities have accepted broad exceptions to obtaining particularized consent.[118]

Nevertheless, predictive analytics in both health care and policing represent a similar general societal bargain that may undergo recurring re-evaluation as technology develops; that is, we accept a small risk that certain privacy interests of individuals are materially violated (either in the improper disclosure of health information or the creation of an excessively robust police profile) in order to receive the benefits offered by big data. What is more, while the contours of this bargain are partially shaped under a framework of political accountability, through oversight and regulation, individuals are largely forced participants: the data collected by police are often the inevitable outgrowths of living in modern society,[119] and people often cannot always choose how to receive vital health care.[120] While the point at which an acceptable tradeoff becomes unacceptable may be different in medicine and policing, the societal decision-making mechanisms actually bear a strong resemblance.[121]

[116] Cohen, *Duty to Share*, *supra* note 48, at 293.

[117] *See, e.g.*, PERRY ET AL., *supra* note 13, at 84.

[118] One reader valuably suggested to us the nature of this tradeoff takes a different sort of form than with health care: the very notion of privacy is both simpler and more robust in the medical setting, whereas when it comes to policing, what we mean by privacy and our willingness to subordinate it to other values seems more complex.

[119] *See generally* Smith v. Maryland, 442 U.S. 735, 750-51 (1979) (Marshall, J., dissenting) (framing privacy expectations as contingent upon "the risks he should be forced to assume in a free and open society"). On the other side of this coin, there are also times where the public's access to the data causes problems and it may be socially desirable for the police to keep certain information (e.g., body camera footage) private in order to curb unintentional collateral consequences (e.g., employability, credit, housing, and the like).

[120] As discussed above, in the health care context there remains much more of a live debate about whether one should *both* be able to receive health care *and* deny the sharing of one's data, or at least set parameters on how that data is shared. The debate seems much less alive when it comes to policing — it is taken for granted that the result of police observation of one's behaviors will become part of a common information pool.

[121] Interestingly, this resemblance perhaps starts from different paradigms. Cops

G. Transparency, Circumvention, and Trade Secrecy

As discussed throughout, transparency is key to the effective adoption of predictive analytics within both health care and policing. At the same time, most big data systems are highly opaque. Neil Richards and Jonathan King pointedly label this phenomenon the "Transparency Paradox": despite big data's "promises to use this data to make the world more transparent" in fact "its collection is invisible, and its tools and techniques are opaque, shrouded by layers of physical, legal, and technical privacy by design"; that is, "[i]f big data spells the end of privacy, then why is the big data revolution occurring mostly in secret?"[122]

The reasons for limited public disclosure differ in the contexts of policing and health care. The police face a range of unintended consequences of too much transparency that do not similarly imperil medical professionals. When it comes to openness, it is desirable for physicians and health care workers "to explain [to patients] whatever predictive analytics development and evaluation they are undergoing and the likely benefits and risks."[123] The big constraints relate to systemic complexity, especially (as discussed above) concerning machine learning and (as discussed below) trade secrecy.

When it comes to law enforcement, incautious disclosure of predictive policing tactics, without adequate regard for its consequences, may prove entirely self-defeating.[124] The Internal Revenue Service, for example, employs a proprietary algorithm to decide which of the millions of tax returns should be annually audited.[125] Some regulatory agencies are currently working on developing algorithms that can detect probable fraud from the sorts of language used in a company's financial or proxy statements.[126] Disclosure here, as to the sort of behavior the IRS finds suspicious or the kind of language that may unintentionally indicate fraud, would materially undermine the law enforcement purposes of the software. As applied to policing, imagine a situation where a department was

are public servants who deal largely with public information. Doctors owe fiduciary obligations to their patients and rely on confidential information from those patients.

[122] Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 42-43 (2013).

[123] Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1144.

[124] *See generally* William J. Stuntz, *Secret Service: Against Privacy and Transparency*, NEW REPUBLIC, Apr. 17, 2006, at 12 (arguing that imprudent disclosures are the core problem within government information collection).

[125] Simmons, *supra* note 24, at 957.

[126] *See* Rich, *supra* note 17, at 875-76.

required to announce the locations of its determined "hot spots" for a neighborhood: any self-respecting drug dealer would pick up shop and move 500 feet in another direction.[127] Within the intelligence community, the importance of preserving sources and methods has long been recognized by the courts.[128] The same sort of risks apply to imprudent transparency for law enforcement, where criminals and criminal networks may quickly learn how to "game the system" once the police tip their hands.[129] For predictive policing, transparency is likely better seen as a means to an end — be it better methodologies or political legitimacy — rather than a good in itself.[130]

The threat of over-disclosure seems more foreign in the health care landscape in part because of the different configuration of the parties. In health care there is largely an alignment (albeit not a perfect alignment) of interest between the "users" of the predictive algorithm and its "subjects." The system, when it works, is aimed to improve the

[127] In addition, consider the contrast between a "risk score" in health care and a police profile that lands someone on a "heat list." Each are derived from a predictive analytics model. But while disclosing the rationale for a "risk score" is important for aiding patients and maintaining a choice architecture, see Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1145, doing the same for a suspected offender would likely provide a criminal network a guidebook to escaping police notice.

[128] *See, e.g.*, United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."). To be sure, these kinds of arguments against disclosure will not be appropriate for all policy forms of predictive policing. When disclosure does not lead to circumvention, for example, the argument for disclosure is much weaker. Consider, for example, a recent court order requiring disclosure of the code underlying the Forensic Statistical Tool used by New York police to analyze complex DNA evidence, in order to enable challenges to the use of the tool in court. *See* Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence. It is hard to see that disclosure as circumvention-enabling.

[129] *See* Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 361 (2008) ("The reason for the secrecy of the [data mining] programs is that exposing the algorithms and patterns that trigger identification as a possible future terrorist will tip off terrorists about what behaviors to avoid.").

[130] *See* Weisburd, *supra* note 32, at 678 ("Consensus and transparency, coupled with a tight focus on high-crime locations, can enhance the legitimacy of police intrusions that are necessary to intercept criminals for violating 'risk laws,' such as those against carrying guns or driving while intoxicated."); *cf.* Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 941 (2006) (discussing "open government [as] a means to improve governance rather than an end in itself").

health of patients.[131] Perhaps more importantly, it is not clear that patients would be very capable of "gaming" the system even if they knew how the system worked or, at a high level, its aims. The same is not true of the policing context where the "users" (police) have a more adversarial relationship with at least some of the "subjects" of the system — obviously those who seek to get away with law-breaking, but more subtly those who are innocent but nonetheless picked out by the system for unwanted attention. Moreover, such gamesmanship is a more realistic concern in circumventing the system.

Concerns about gamesmanship should not serve as justifications for complete opacity within policing. Instead departments and stakeholders should endeavor to strike a balance between a level of disclosure that adequately allows for political oversight and buy-in, while also preserving the efficacy of the tools deployed by law enforcement. For instance, police departments may choose to disclose the sorts of datasets they keep on the surrounding community, but withhold specifics regarding the method of collection or the manner in which the information is analyzed.[132] A different solution is to substitute third-party auditing for public disclosure. For instance, "[l]ocal governments can provide independent third parties with responsibilities and powers to review how [big data policing tools] work."[133] Independent boards, although not currently developed,[134] could be an elegant solution to a number of the problems contemplated herein: by pooling expertise (existing practitioners, industry leaders, external observers, etc.) and limiting disclosure, such boards could provide effective oversight without triggering the transparency problems of gamesmanship or trade secrecy.

To that point, when it comes to predictive analytics in health care, attempts to protect intellectual property, especially through trade secrecy, are a big obstacle:

[131] Why not a perfect alignment? Because the users of predictive analytics in health care may have over-determined motivations. In particular, they may be motivated both to improve the health care of specific patients and to reduce the health care costs for the whole population. As the discussion above regarding distributive effects acknowledges, it is also possible for a predictive analytics system to benefit some patients but disadvantage others.

[132] *See* Zarsky, *supra* note 7, at 1563-64.

[133] Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 41 (2016). There may be analogies in other areas as well, such as accounting practices.

[134] *See* Ferguson, *Predictive Policing and Reasonable Suspicion*, *supra* note 22, at 320.

> [M]any big data practices likely fit within trade secret law's expansive definition of "information." Because such practices are typically implemented through software, a big data producer could also obtain trade secret protection over the code that assists experts in carrying out these practices. Moreover, from a practical perspective, secrecy over such information may be even easier to maintain than secrecy over software methods. The recent commentary describing big data's disclosure problem indicates that, unlike software, big data practices cannot be reverse-engineered.[135]

In the medical context, we face a real trade-off between incentives and transparency. Trade secret protection is the most effective intellectual property incentive to drive the development of black-box medicine, but that incentive creates real problems for transparency and oversight.[136] Without a nudge from regulators (or perhaps consumers), such transparency is unlikely to come. One solution is to go for a kind of second-best transparency, through regulatory (or more likely) third-party validation and auditing. For instance, predictive models could be accredited by third parties such as the Joint Commission, or the National Quality Forum could set standards that predictive analytics would have to meet.[137] It is possible that the market for analytics will itself demand such accreditation or validation. If it fails to do so, the Centers for Medicare and Medicaid Services ("CMS") or another health care government funder (or private insurers) could require said accreditation or validation as a condition of reimbursement. It is also possible that a government agency could itself accredit or validate, which might have a benefit of removing worries about regulatory capture, but the FDA thus far has shown no appetite for reviewing software in medical devices and it is not clear what other agency might step up to the plate.[138] The fact that the federal government imposes conditions for reimbursement that are complied with by almost all hospital systems is a distinct inroad for regulatory oversight implementation as compared to the predictive policing contexts. Police departments, as creatures primarily of

[135] Michael Mattioli, *Disclosing Big Data*, 99 MINN. L. REV. 535, 552-53 (2014).

[136] Price, *Big Data, Patents*, *supra* note 8, at 1435-36.

[137] *E.g.*, Cohen et al., *Legal and Ethical Concerns*, *supra* note 4, at 1143; *see also* Price, *Black-Box*, *supra* note 51, at 448.

[138] In a soon-to-be-published paper, Nicholson Price has higher hopes for the FDA in this regard and has suggested that the FDA should provide an information-sharing role to allow collaborative governance by other health-care system actors. *See* Price, *Regulating Black-Box*, *supra* note 52, at 448-54.

municipalities without direct lines of central or even practicable federalized oversight, present a significantly deeper challenge in this regard.

CONCLUSIONS

What can the cop teach the doctor and vice versa? Here are some tentative lessons:

Inevitable Distributive Effects: There will be winners and losers from the adoption of predictive analytic systems in both policing and health care. Of course, there are winners and losers in the status quo small-data practices, and the fact that these practices are currently in existence does not itself give them moral priority. The willingness to recognize model building and implementation as an inherently redistributive enterprise is more apparent on the health care than the policing side. Because the just distribution of health care resources has long been a prominent question for bioethics, there is much more normative thinking on what kinds of trade-offs are morally permissible, as well as more thinking on designing fair processes for resolving trade-offs where moral theory runs out. In an ideal world, some of this thinking could be brought over to the policing space, but there are perhaps prohibitive hurdles in finding consensus metrics for winners and losers, as well as deciphering certain cause-and-effect questions that pertain to policing strategies.

Differences in Political Economy: In health care there is more of a natural alignment between the "users" (hospital systems, doctors) of the predictive algorithm and its "subjects" (patients). Both have shared interests that run fairly deep in improving the health of patients, though admittedly this does not exhaust either party's interest. In policing the "users" (police) have a more adversarial relationship with at least some of the "subjects" of the system — those who seek to get away with law-breaking, but more subtly those who are innocent but nonetheless picked out by the system for unwanted attention. To put the point another way, the introduction of predictive analytics in health care has a redistributive effect but *ex ante* it is harder to know whether and to what extent an individual patient will be a loser or winner from its introduction even when the system is successful. By contrast, many legal scholars and other academics think the winners and losers are more predictable *ex ante* in policing and losers tend to cluster amongst discrete and insular minorities. Elected officials and police departments, alternatively, are more likely to see implementing a predictive policing model as a possible "win-win," rendering better police services that benefit the whole community, even though its actual results are hard to evaluate and widely debated across various stakeholders. These differences, which also intersect with constitutional questions and institutional distrust across actors in the political process, may then require stronger judicial oversight of predictive policing than in the health care context.

Liability as a Check: The potential for liability against health care providers and hospital systems may act as something of a check against overambitious use of predictive analytics in health care.[139] Similar theories of liability are not immediately available for those who are aggrieved by predictive analytics used in policing, who likely will have to resort to a more general political process, petitioning representatives or creating public pressure, instead of demanding change from police departments themselves through market forces (such as when selecting a different doctor or hospital) or lawsuits. Perhaps it would be good if we moved towards more generalized theories of "predictive negligence" that could be used across life domains that adopt predictive analytics. It is hard to know what would be better, but, in any event, such an approach seems very unlikely in the foreseeable future. Where liability theories (including the potential of discovery through litigation) are less available, as in policing, it is reasonable to demand more transparency and governance oversight.

Education and Oversight: With the implementation of predictive analytics in both the health care and policing contexts, the understanding of the "subjects" — the patients and the public — is crucial to avoid widespread resistance. For this reason, the best practices involve community wide consultation and, at least in the health care context, notification if not true informed consent. More generally, the fiduciary relationship between physician and patient all push towards more consensual and open dialogue. By contrast, the options for richer disclosure are somewhat more limited in the policing context due to the fear that disclosure will lead to circumvention. In both contexts, trade secrecy and the fact that these algorithms are typically developed by for-profit commercial entities also imperil disclosure. Finally, when it comes to machine-learning forms of predictive analytics true disclosure may just be impossible. Where fuller disclosure is not possible, the second-best solution in both contexts is a move to third-party auditing and verification.

[139] The flipside fear is that too much of a threat of liability will be a push towards too little ambition on the part of hospitals. Unlike Goldilocks, it seems improbable that courts will get things "just right" in developing the tort doctrine, so one needs to make a distributional decision whether Type 1 or Type 2 error is the more important to avoid.

Because of the role of federal funding in health care, there is a surer path to mandate that result than in the policing context. Nevertheless, federal and state regulators should consider to what extent, through funding or regulation, they can steer police departments using predictive analytics towards third-party verification and auditing.

Making the Privacy Bargain: Relatedly, both fields revolve around tradeoffs where individuals sacrifice certain privacy interests in exchange for broader, systemic improvements. Interestingly, this bargain is somewhat compelled in each context. For policing, individuals inevitably disclose tremendous amounts of personal information as a feature of modern society. In health care, most patients are largely unaware of the use of their health care data and, even when informed, may not have many options to prioritize a number of factors in making choices between providers ahead of the use of their de-identified data. For these tradeoffs to remain sustainable into the future, they will need to maintain a social legitimacy derived from public accountability and generalized consent. In health care, the hurdles for doing so are lower: disclosure is often in the interest of hospitals and doctors, and institutional trust is higher. Therefore, we expect that the health care space will undertake these exercises well before policing, and therefore can provide a possible template for (a) explaining complex technological concepts to the public, and (b) promoting comfort with the proposed privacy bargain. In turn, for law enforcement to effectively employ these lessons, they will need to curb instinctual preferences for over-classification and welcome certain structural oversight.

Predictive analytics is one of the most exciting technological changes, to both policing and health care, in a long time. Tomorrow's precinct and hospital may look radically different from the way they do today and we may in the future recoil at today's methods just as today we react badly to accounts of trepanation, bloodletting, phrenology, and bertillion identification. Or not. As is sometimes attributed to Yogi Berra, "[i]t's tough to make predictions, especially about the future."[140] But while at a surface level one might have thought there was little room for dialogue between medicine and policing, in this Essay we have tried to show the way each has a lot to learn from the other when it comes to legal and normative thinking about predictive analytics.

[140] *E.g.*, CAROL S. STEIKER & JORDAN M. STEIKER, COURTING DEATH: THE SUPREME COURT AND CAPITAL PUNISHMENT 289 (2016).