I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Predictive Analytics Law and Policy: A New Field Emerges

DENNIS HIRSCH*

The symposium papers in this volume focus on predictive analytics law and policy. What is "predictive analytics"? According to one definition, it is "[t]echnology that learns from past experience (data) to predict the future behavior of individuals in order to drive better decisions."[1] An example will serve to illustrate.

Several years ago, credit card companies sought to identify potential customers who would be likely to pay their credit card bills rather than default on them.[2] In predictive analytics this desired quality, the one that the analysis is trying to predict, is referred to as the "target variable." The companies had a large database of information about current and past customers, their purchases and their payment records. But they didn't want to know about its about its current or past customers. They wanted to know about potential future customers and whether they would be likely to pay or to default. They set about analyzing their store of "big data" to see if they could find a pattern. Did those who paid their credit card bills purchase certain items that those who defaulted did not? In other words, could the companies find a "correlation" between the purchase

* Professor, The Ohio State University Michael E. Moritz College of Law; Professor, Capital University Law School.

[1] ERIC SIEGEL, PREDICTIVE ANALYTICS 15 (2016).

[2] Jonathan Shaw, *Why "Big Data" Is a Big Deal*, HARVARD MAG., Mar.-Apr. 2014, at 30, 31 ("Credit-card companies have found unusual associations in the course of mining data to evaluate the risk of default: people who buy anti-scuff pads for their furniture, for example, are highly likely to make their payments.").

of certain items and the paying of one's credit card bills? If so, it could take this correlation and apply it prospectively to predict which potential customers would be likely to pay their bills.

The companies did not know what type of purchases they were looking for. They had no hypothesis about the types of purchases that would predict the likelihood of paying one's credit card bills. They looked for their answer in the data. The analysis showed those who purchased anti-scuff pads to attach to the legs of their furniture defaulted at a much lower rate than those who did not.[3] This pattern can be formulated as a simple algorithm, a "step-by-step procedure for solving a problem or accomplishing some end."[4] Here, the algorithm is: if a person purchases furniture anti-scuff pads, then that person is unlikely to default on his or her credit card debts. The analysis did not explain why this was so. It could have been that those who take care of their floors show the same responsibility with respect to their credit card bills. Or, it could have been that it is those who have nice, wooden floors that generally furniture anti-scuff pads, and that these individuals are wealthier or have a different character than the general population. Or, it could have been something else entirely. The analysis did not say. But it did show that those who purchased furniture anti-scuff pads were highly likely to pay their credit card bills rather than default on them. Stated a bit differently, it showed that the correlating item (purchase of furniture anti-scuff pads) was a good "proxy" for the target variable (low credit default risk). The credit card companies presumably used this information to target their credit card ads to these individuals.

This illustrates predictive analytics in a nutshell. The analysis begins with the item that it wants to predict – the "target variable." It then consults a large data set that includes the target variable as well as many other data points. It looks retrospectively at this data set and asks: in the past, what other data points have correlated to the target variable? It then takes this "proxy" (here, the purchase of furniture anti-scuff pads) and applies it prospectively so as to *predict* the presence of the target variable. In the final step, it acts on this insight. This is the sense in which predictive analytics is "[t]echnology that

---

[3] *Id.*

[4] *Algorithm*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/algorithm [https://perma.cc/9SBG-VGE5].

learns from past experience (data) to predict the future behavior of individuals in order to drive better decisions."[5]

Such an analysis, grounded in credit card companies' database of customer purchases, is powerful. But imagine what one could learn from analyzing a dataset that also included search queries, web surfing history, social media activity, use of electricity, locations frequented (as revealed by one's cell phone), public records and the many other data trails that we increasingly leave as we travel through life. Think of all the unexpected, interesting correlations that one could find for predicting target variables. Think of how precise those predictions, which link together multiple attributes into a single proxy, would be. This is the world of predictive analytics, the world in which we all now live.

THE BENEFITS OF PREDICTIVE ANALYTICS

Anyone who has received an Amazon book recommendation has experienced predictive analytics in action. Amazon bases its recommendations on correlations in its database of purchases (persons who bought or looked at book A also bought book B) that allow it to make predictions: if someone purchases or looks at book A, then they are likely also to be interested in book B.[6] While some find such recommendations to be "creepy,"[7] many others find them to be useful. They have certainly been useful for Amazon, which attributes a third of its sales to its recommendation and personalization systems.[8]

Predictive analytics has many other beneficial applications beyond marketing. Medical researchers use it to predict which medicines or treatments are likely to work best for a patient with specific characteristics.[9] Educators use it to predict which students are at risk

---

[5] SIEGEL, *supra* note 1, at 15.

[6] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK 50-51 (2013).

[7] Jules Polonetsky & Omer Tene, *A Theory of the Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 61 (2013).

[8] MAYER-SCHÖNBERGER & CUKIER, *supra* note 6, at 52.

[9] PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 13 (2014), https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/F8CB-XUYW].

of dropping out and to target additional support and resources to them.[10] Banks use it to predict which transactions are likely to be fraudulent.[11] Big data analytics is rapidly spreading throughout the economy and society at large and is generating many important benefits.

THE RISKS OF PREDICTIVE ANALYTICS

Outside of the law and policy field, much of the writing on predictive analytics focuses on these benefits. This Symposium makes an important contribution by focusing on the risks of predictive analytics and how best to address them. Predictive analytics poses four main types of risks: (1) privacy risk; (2) bias risk; (3) error/Due Process risk; and (4) exploitation risk.

Privacy risk

Just as predictive analytics can infer whether a person is a good credit risk, so it can infer whether a person is gay, at risk of heart disease or diabetes, a Republican, and much other sensitive data in which individuals have a privacy interest. Those who infer this information may reveal it, either intentionally or inadvertently, to others. In one well-known example, Target used data analytics to identify which of its customers was pregnant, marketed baby-related goods to them and, in so doing, tipped a father off to the fact that his fifteen-year-old daughter was pregnant.[12] Such unauthorized disclosure of highly sensitive information is a classic privacy injury.

Bias risk

Predictive analytics can also result in harmful bias against protected classes. Anti-discrimination law distinguishes between two types of harmful discrimination: "disparate treatment," in which one

---

[10] *Id.* at 12.

[11] EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 39 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/DGD4-MPUG].

[12] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

intentionally discriminates against another to their disadvantage because of that person's membership in a protected class; and "disparate impact" in which facially neutral policies have an unjustified, disadvantageous impact on the members of a protected class, regardless of intent.[13] Predictive analytics can lead to both types of harmful discrimination, particularly when businesses employ it to determine eligibility for loans, jobs, or other important life opportunities and goods. For example, an employer could use Target's pregnancy prediction method (or something like it) to determine which female job applicants were likely to be pregnant and then deny interviews to them. This intentional act would constitute disparate treatment of the members of a protected class and would violate employment discrimination law.[14] But applicants and anti-discrimination authorities would find it hard to detect the violation given that the company did not ask an illegal question or otherwise make its intentions known.

Predictive analytics can also produce disparate impact discrimination. Returning to anti-scuff furniture pads, it is possible that one religious or racial group purchases this item much more frequently than others. Purchasing anti-scuff pads would then correlate, not only to being a good credit risk, but to being a member of a particular religion or race. Use of this proxy to allocate credit cards creates a disparate negative impact on certain religions' or races' access to credit. The same thing could occur with the use of predictive analytics to allocate loans more generally, jobs, insurance, admission to schools, and other important goods. These impacts may, or may not, violate anti-discrimination law, depending on the degree of the impact, the business justification for the sorting, and the existence of reasonable alternatives for achieving this business end.[15] But they could further take us down the path to a society in which certain races or religious groups have more access to important life opportunities and goods than others.

---

[13] Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact,* 104 CAL. L. REV. 671, 694 (2016).

[14] *See generally* Civil Rights Act of 1964 tit. VII, Pub. L. No. 88-352, 78 Stat. 241 (as amended, 42 U.S.C. § 2000e-2(2) (unlawful for employer to deny employment opportunities because of or on the basis of an individual's sex); *id.* § 2000e(k) (defining "because of or on the basis of an individual's sex" to include "because of or on the basis of pregnancy, childbirth, or related medical conditions.")).

[15] *See generally* Tal Zarsky, *Understanding Discrimination in the Scored Society,* 89 WASH. L. REV. 1375 (2014); Barocas & Selbst, *supra* note 13, at 701-12.

Biased data sets can produce harmful discrimination. For example, assume that workplace bias makes it easier for men to succeed as high-level corporate executives than for women to do so. This would lead the existing set of successful high-level corporate executives to be disproportionately male. An analysis that used this data to identify the characteristics of a successful high-level corporate executive might well yield male gender as a predictive proxy. This could then provide a data-driven, "objective" basis for hiring more men for high-level executive positions, thereby masking and perpetuating the human bias inherent in the data itself. This is the kind of dynamic that Cathy O'Neil in her book *Weapons of Math Destruction* refers to as a "pernicious . . . feedback loop" in which "the model itself contributes to a toxic cycle and helps to perpetuate it."[16]

Error risk

The third category is the risk of error or, as it can also be conceptualized, risk to due process. Faulty facts and flawed algorithms can lead to erroneous predictions that harm people. For example, analytics might incorrectly predict that someone is likely to commit acts of terrorism and place that person on the no-fly list even though, in fact, the individual has no propensity to commit such acts.[17] This could seriously impinge on the person's right to travel. Of course, human decision-makers commit errors as well. The mere fact that the predictive analytics in this instance is wrong does not, in and of itself, make it any worse than other methods of determining who belongs on the no-fly list.

The real problem is that the predictive analytics' errors are invisible to those they affect. A person erroneously placed on the no-fly list has no way of knowing what facts or decision-making process led to the result. From the individual's vantage point, predictive analytics is a "black box"[18] that the person has great difficulty challenging. Thus, the risk is not just one of error. It is a diminishing of the individual's ability to know about and challenge that error. It is

---

[16] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 27 (2016).

[17] Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1788-92 (2016).

[18] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3 (2015) (using "black box" as a metaphor for predictive analytics-based decision-making).

the risk of living in a Kafkaesque society in which unseen decision-makers make unexplained decisions that affect our lives profoundly. It is a risk to due process, not simply a risk of error.[19]

Exploitation risk

The fourth major risk is the use of predictive analytics to identify those who are vulnerable in order to exploit these vulnerabilities. Certain for-profit educational institutions are some of the worst abusers. They use predictive analytics to identify individuals who are isolated, have low self-esteem, have experienced a recent death in the family, or have dead end jobs. They then target ads to those individuals promising them a bright future if they take out loans to pay for expensive private education.[20] These ads "pinpoint people in great need and sell them on false or over-priced promises. They find inequality and feast on it."[21] Of course, snake-oil salesmen and others have preyed on human vulnerability for generations. What has changed is use of predictive analytics to infer such vulnerabilities from the mass of data that each of us releases as a consequence of living in a digital society. It is as if the predators were given a super power that allowed them to see through our protective shells and identify each of our most vulnerable spots, and then to try to take advantage of it. Such behavior puts many people at risk, not just those who are members of protected classes. It is better characterized, not as bias, but as exploitative behavior that uses predictive analytics to take advantage of vulnerable populations.

In sum, predictive analytics poses four major types of risks: privacy risk, bias risk, error/due process risk, and exploitation risk. The challenge is to design and implement this field in a way that will maximize big data's benefits, and reduce its risks, so that the former greatly outweigh the latter.

This brings us to the topic of this Symposium, which is how to design laws and policies to achieve this end. The answers are far from

---

[19] *See generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. L. REV. 1249, 1251-58 (2008) (computer-based decision-making by-passes traditional Due Process protections); Kate Crawford & Jason Schultz, *Big Data and Due Process: Towards a Framework to Address Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014) (big data analytics frustrates Due Process norms).

[20] O'NEIL, *supra* note 16, at 70-81.

[21] *Id.* at 70.

clear. To begin with, predictive analytics poses interesting new challenges for the traditional privacy regulatory approach of providing individuals with advance notice of and choice over the collection and use of their personal data. It raises questions such as: How can organizations provide individuals with notice of and choice over collection when data collection is so wide-spread and continuous? How can they provide individuals with notice of and choice over the purpose to which they intend to put the data when they frequently do not know what this use will be until after the correlations are found and the data "speaks"? What does it mean to protect privacy in such an environment, and how can law and policy best achieve this?

With respect to bias, the solution to intentional disparate treatment of protected classes is straightforward enough. We need to find ways to detect and stop it. But what about disparate impact? How much impact must there be to require legal intervention, and when should predictive analytics' business and other benefits be sufficient to justify it? Should traditional anti-discrimination law be our guide? Or, do we need an updated framework capable of handling new, data-driven forms of bias? What about biased data sets and data analytics' propensity incorporate them and perpetuate the bias they contain? How are we to detect and correct such data sets? How can we construct the counter-factual of an unbiased data set?[22]

With respect to Due Process, should organizations give individuals access to the data they hold about them and allow them to challenge whether, in fact, they possess the correlating attribute that led the machine to categorize them in a particular way? Should they give individuals access to the algorithm itself and allow them to challenge it? What about the company's proprietary interest in the algorithm that it has developed? Does trade secrecy trump Due Process in this context? It not, how might they be harmonized?

Finally, how should we distinguish between appropriate use of predictive analytics and "exploitative" use? What constitutes a vulnerable population? Who should draw this line, and where should they draw it? In each of the four risk areas, predictive analytics poses fascinating questions for law and policy.

A growing number of legal scholars are engaging with these and related questions. When Professor Peter Shane, 2016-2017 Symposium Editor Sara Coulter, and I came together to discuss a theme for this year's I/S Symposium, we looked at this body of work

---

[22] *See* Barocas & Selbst, *supra* note 13, at 717.

and thought: What we are seeing here is the emergence of a new field of legal scholarship. The field spans many substantive areas. Some scholars write about predictive analytics in education; others, in the field of medicine; others, marketing, or law enforcement. But all, in some way, come back to the four main areas of risk—privacy, bias, error and exploitation—and how law and policy should govern them.

Wouldn't it be exciting to bring these scholars together so that they can share ideas and, together, begin to map out the contours of this growing field and identify its core themes? This idea led to the Symposium. The *I/S Journal* has been very fortunate to be able to bring together some of the most thoughtful voices in this young field. Each has produced a paper from that conveys that person's own, unique vantage point.

The purpose of this volume is, first, to present these interesting and insightful works. But it also seeks to do more. By juxtaposing these related, yet independent inquiries, this Symposium seeks to reveal the risks that cut across the various fields of predictive analytics and allow consideration of whether the solutions reached in one area might also work in others. In short, it seeks to enable the reader to see and think about the field of predictive analytics law and policy and to begin to map its themes and contours. If it succeeds, it will take a small step forward towards the establishment of this emerging and exciting new field.