

Law and Technology

Automated Prediction: Perception, Law, and Policy

A few predictions about predictions.

THE U.S. GOVERNMENT receives more than 100 million tax returns each year.³ Based on previous behavioral patterns, computers select the very few tax returns that are subjected to the much-feared auditing process. Similarly, millions of packages and individuals cross international borders. Governments are considering the use of computerized algorithms for the selection of parcels and people for additional scrutiny. In addition, governments are considering automated prediction for a wide range of various tasks, from insider trading detection to fighting and preventing violent crimes. Generally, governments consider automated predictions when personal information about individuals is available. They are further motivated to take such action when the antisocial activities they strive to block are difficult and costly to detect.

Automated prediction is also generating interest in the context of detecting and preventing terrorist activities. Here, an additional factor enters the equation: the devastating effects of successful attacks in terms of human casualties. These effects, at times, lead to rash policy decisions, as well as radical changes in public opinion. Some academics and policymakers are well aware of these dynamics, and call for exercising great caution when examining the role of new and possibly invasive policy measures in this context. They are right to do so. However, in some cases, automated prediction is



Official seal of the decommissioned U.S. Information Awareness Office, which funded research and development of the canceled Total Information Awareness initiative.

indeed an appropriate measure, given its hidden benefits.

Automated prediction is perceived as problematic and even frightening by a large percentage of the general public. This common visceral response is not always rational and accurate, yet it is backed by several relevant legal concepts. Automated prediction deserves a closer look, as it might promote important social objectives, such as equality and fairness. Reexamining automated prediction should lead to a broader role for these practices in modern government. Legal impediments blocking some of these practices should be re-

thought and perhaps removed, even in view of the negative perception by the general public.

In the previous decade, the interplay between law and public opinion in the context of automated prediction played out in the U.S. public debate regarding the Total Information Awareness initiative. This project was intended to structure massive datasets that would be used for automated identification of terrorist activity. Due to popular pressure, this ambitious project was canceled. It is widely suspected, however, that similar projects are still being carried out. Indeed, in

early 2012, the *New York Times* reported on the expansion of predictive automation to assist in ongoing efforts to detect and prevent terrorism.¹

The notion of automated prediction by government is destined to meet even greater resistance in Europe. But there too, pressure will mount for the adoption of some predictive measures. France, for instance, is already feeling the heat. Following its failure to preempt the March 2012 terrorist attack in Toulouse, sources noted this might have resulted from the lack of automated processes for analyzing personal information.² Such allegations will motivate agencies in Europe to push for allowing a greater role for automated prediction.

Before proceeding to establish the proper role of automated predictive modeling and its relation with law and public opinion, we must consider crucial preliminary questions: Does automated prediction indeed “work”? Can it identify risks effectively and efficiently without wrongfully engaging the innocent and ignoring the guilty? Proponents of automated prediction will be quick to note its success in the commercial realm. Here, marketers and vendors are able to predict their customers’ needs with astonishing accuracy, at times even before the customers acknowledge their needs on their own.³ However, it is unclear whether success will follow in the governmental context, and measuring such success is a challenge of its own. For the sake of this argument, let us assume that in some contexts automated predictions prove effective. It is within these specific contexts that we must move forward and examine whether such practices must be implemented, regardless of current public opinion and while challenging the existing legal framework.

Public Perception, Technology, and Law

The public’s negative response to automated prediction can be better understood after examining the mechanics of this process and the tech-

Proponents of automated prediction will be quick to note its success in the commercial realm.

nologies that enable it. First, the process is made possible by the ease with which personal information is collected, saved, and aggregated, at times with other intentions in mind. Second, the process is enabled by data mining tools. Data mining brings with it the promise of finding hidden trends within the data; trends the analysts did not even know to look for. It is also an automated process, which is not driven by an initial hypothesis.

These two central elements, personal data management and automation, generate public anxiety. Such anxiety is reflected in two fundamental legal principles. These principles are enshrined, among others, in the European Data Protection Directive^b (and some U.S. laws) and are compromised by automated prediction. The first legal principle states that personal information collected for one objective should not be utilized toward another without the individual’s consent. However, in almost all cases, the information used in the automated predictive process was gathered with other intentions in mind. The intention to carry out predictive analyses was not conveyed to the relevant data subjects. The theory behind this rule is that individuals should have some control over personal information pertaining to them. The second legal principle, as noted in Article 15 of the European Directive (and other European national laws), states that automated processes that have a substantial impact on an

individual are forbidden unless they include an element of human review. This principle could be backed by several theories. One can argue that an automated process that directly impacts an individual is undignified. Or, that such a process might be riddled with errors that will go unnoticed. We must remember, however, that both of these legal principles have exceptions. As I now argue, when automated prediction is efficient and effective, these exceptions should be considered.

Automated Prediction, Human Discretion, Errors, and Biases

When considering automated prediction, both legal analysis and public opinion are missing a crucial point. Automated prediction actually *promotes* important social objectives that both law and public opinion hold dear—fairness and equality. To understand this point, we need to look beyond the existing legal rules and basic intuitions mentioned here. We must confront one of automated prediction’s alleged major flaws and perhaps the source of the legal rules and the public attitudes mentioned earlier: the fact that in some instances individuals would be wrongfully suspected and engaged due to a computer error. Indeed, a process that makes arbitrary errors is problematic. A system that subjects individuals to such errors is both unfair and undignified. The fact that this process is computer-driven will probably make things worse. Individuals are used to second-guessing decisions of bureaucrats and officers but they surprisingly accept without question decisions made by computers.

To fully understand this concern, consider it in light of its most immediate alternative, a system in which decisions are made by humans (which indeed might rely on computerized assistance and even recommendations, yet still includes a substantial human component). Here as well, errors will follow. Yet these will be errors that result from the shortcomings of human discretion. Many would prefer dealing with this second set of errors. The relevant decision maker could be questioned and the faulty logic quickly located. Furthermore, the implicated individual would be provided with re-

a For an account of these practices as carried out in the U.S. by Target, see Duhigg, C., “How Companies Learn Your Secrets.” *New York Times* (Feb. 16, 2012); http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&ref=charlesduhigg.

b Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

dress and future similar problems will be averted. Thus, the public and legal attitudes against automated prediction seem to be justified.

Yet there is a substantial shortcoming in this human-driven alternative strategy, which might eclipse all the advantages of human discretion and lead us back to automated prediction as a preferred option—the notion of *hidden biases*. In many instances, human errors are not merely arbitrary. Rather, they result from systematic (while possibly subconscious) biases. Recent studies indicate that subconscious biases against minorities still plague individuals and their decision-making process. At times, decision makers (both in the back office and the field) discriminate against minorities when making discretion-based decisions, even unintentionally. Given these subconscious trends of behavior, a discretion-based process is structurally prone to these forms of errors. On the other hand, automation introduces a surprising benefit. By limiting the role of human discretion and intuition and relying upon computer-driven decisions this process protects minorities and other weaker groups. Therefore, a shift to automated predictive modeling might be affecting different segments of society in predictable, yet different ways.

It should be noted that the “hidden bias problem” might migrate to the automated realm. Automated decision making relies upon existing datasets, which are often biased regarding minorities, given years of unbalanced data collection and other systematic flaws. Restricting the use of problematic factors and their proxies, as well as other innovative solutions that systematically attempt to correct data outputs, can potentially mitigate these concerns.

Returning to our discussion regarding the interplay between public opinion and law, and with the novel intuition regarding the hidden benefits of automated predictions in mind, our analysis must examine how prediction might be impacting the segmented public’s opinion and what are the implications of these findings.

For members of the powerful majority, a shift toward an automated model might prove to be a disadvantage. In a discretion-based process, the chance

For members of the powerful majority, a shift toward an automated model might prove to be a disadvantage.

of a member of the powerful majority to be wrongfully singled out is low. Even if selected for further scrutiny, members of this group can try to appeal to the reason of another individual. This appeal would involve a human decision-making process, thus again involving subconscious biases. In these cases, there is a better chance the subconsciously biased decision maker will act in their favor. Therefore, the powerful majority’s vocal discontent with automated prediction is rational, yet socially unacceptable.

However, things are quite different for members of a minority group. For these individuals, human discretion is not always a warm human touch, but at times a cold discriminating shoulder. The automated process increases the chances of blind justice. While society installed various safeguards against these forms of governmental discrimination, such measures still fail to limit the impact of unintentional (and even subconscious) biases. Automated prediction might be the most powerful solution to the problems of such hidden discrimination—a solution the unpopularity of this measure should not block.

Conclusion

This analysis argues that the negative opinion flowing from at least part of the public—the powerful majority—regarding automated prediction should be ignored. One might go further to note that the broad anti-automated prediction sentiment generated through the media is merely a manipulative ploy intended to maintain the existing social structure and ensure the “haves” continue to benefit from structural advantages. Even with-

out accepting this final radical view, we must beware of popular calls to limit the use of predictive automation and further examine if they reflect the interests and opinions of all.

With these insights in mind, we return to the role of law. This brief analysis shows that we must be more open-minded to the possibility of applying automated prediction by governments, and structure our laws accordingly. Current legal principles are unfriendly to automated prediction models for important reasons: most notably, the need to maintain control over personal information and assure individual dignity. Yet given the ability of these models to promote equality and fairness, this attitude should perhaps be reconsidered.

Law has additional important roles in addressing numerous difficult questions that will arise when applying automated prediction measures to various governmental tasks. One important role would call for limiting the use of the automated prediction tools to the contexts they were approved for, while blocking them from “creeping” into other realms. Another role concerns transparency. The inner workings of predictive modeling are usually kept opaque to avoid gaming the systems and to protect trade secrets. They are also complex. Rendering them transparent is a serious challenge; this challenge can be met through proper planning of disclosure processes.

Promoting and assuring the success of automated prediction modeling is a difficult task. Yet given the possible benefits pointed out in this column, it is worth a try. ■

References

1. Savage, C. U.S. relaxes limits on use of data in terror analysis. *New York Times* (Mar. 22, 2012); <http://www.nytimes.com/2012/03/23/us/politics/us-moves-to-relax-some-restrictions-for-counterterrorism-analysis.html>.
2. Sayare, S. March 22, 2012. Suspect in French killings slain as police storm apartment after 30-hour siege. *New York Times* (Mar. 22, 2012); http://www.nytimes.com/2012/03/23/world/europe/mohammed-merah-toulouse-shooting-suspect-french-police-standoff.html?pagewanted=1&_r=1&adxnlnx=1332615795-XCnSDQaTfcppBTBhFdrnBQ.
3. United States Census Bureau. Table 480. Internal Revenue Gross Collections by Type of Tax: 2005 to 2010; <http://www.census.gov/compendia/statab/2012/tables/12s0481.pdf>.

Tal Z. Zarsky (tzarsky@law.haifa.ac.il) is a senior lecturer in the Faculty of Law at the University of Haifa, Israel. The ideas presented in this column are further developed in Zarsky, T.Z., “Governmental Data Mining and its Alternatives.” *Penn State Law Review* 116, (2011), 285–330.

Copyright held by author.