Prediction, Preemption, Presumption: The Path of Law After the Computational Turn*

Ian Kerr[1]

*This is a draft version of the article.
As such, the author requests that permission be sought prior to citation.

> *For the rational study of law the blackletter man may be the man of the present but the man of the future is the man of statistics and the master of economics.*
>
> Oliver Wendell Holmes Jr.,
> *The Path of Law* (1897)

1. INTRODUCTION

When I was first asked for a contribution to this volume, I decided to challenge myself to a game of *Digital Russian Roulette*. I wondered what result Google's predictive algorithm would generate as the theoretical foundation for the article that I was about to write on predictive computational techniques and their jurisprudential implications. Plugging the terms: 'prediction', 'computation', 'law' and 'theory' into Google, I promised myself that I would focus this chapter on whatever subject matter popped up when I clicked on the '*I'm Feeling Lucky*' search feature.

So there I was, thanks to Google's predictive algorithm, visiting a Wikipedia page on the jurisprudence of Oliver Wendell Holmes Jr. (Wikipedia, 2011). Google done good. Perhaps America's most famous jurist, Holmes was clearly fascinated by the power of predictions and the predictive stance. So much so that he made prediction the centerpiece of his own prophecies regarding the future of legal education: 'The object of our study, then, is prediction, the

[1] Acknowledgement footnote

prediction of the incidence of the public force through the instrumentality of the courts' (Holmes, 1897: 457).

Given his historical role in promoting the skill of prediction to aspiring lawyers and legal educators, one cannot help but wonder what Holmes might have thought of the proliferation of predictive technologies and probabilistic techniques currently under research and development within the legal domain. Would he have approved of the legal predictions generated by expert systems software that provide efficient, affordable, computerized legal advice as an alternative to human lawyers?[2] What about the use of argument schemes and other machine learning techniques in the growing field of 'artificial intelligence and the law' (Prakken, 2006) —seeking to make computers, rather than judges, the oracles of the law?

Although these were not live issues in Holmes's time,[3] contemporary legal theorists cannot easily ignore such questions. We are living in the kneecap of technology's exponential growth curve, with a flight trajectory limited more by our imaginations than the physical constraints upon Moore's Law.[4] We are also knee-deep in what some have called 'the computational turn' (Hildebrandt, 2011) wherein innovations in storage capacity, data aggregation techniques and cross-contextual linkability enable new forms of idiopathic predictions. Opaque, anticipatory algorithms and social graphs allow inferences to be drawn about people and their preferences. These inferences may be accurate (or not), without our knowing exactly why.

One might say that our *information society* has swallowed whole Oliver Wendell Holmes Jr.'s predictive pill—except that our expansive social investment in predictive techniques extends well beyond the bounds of predicting, 'what the courts will do in fact' (Holmes, 1897: 457). What Holmes said more than a century and a

[2] Advertising for programs such as Quicken Legal Business Pro tells potential consumers that one does not require an attorney to run a small business, as all the required paperwork is included with the software package (Nolo, 2010).

[3] Though his contemporaries, Warren and Brandeis, had recognized the future implications of foundational information technologies, such as snapshot photography, a decade prior (Warren and Brandeis, 1890).

[4] More than 40 years ago, Intel co-founder Gordon Moore observed that computer processing power had doubled about every two years from 1957 to 1965 and predicted that it would continue to do so until at least 2020 (Moore, 1965). In his Law of Accelerated Returns, futurist Ray Kurzweil predicted that this trajectory will continue to evolve across new paradigms in computing once the physical limitations of the integrated chip have been exhausted (Kurzweil, 2001).

decade ago about the 'body of reports, of treatises, and of statutes in the United States and in England, extending back for six hundred years, and now increasing annually by hundreds' (Holmes, 1897: 457) can now be said of the entire global trade in personal information, fueled by emerging techniques in computer and information science, such as KDD:[5]

> In these sibylline leaves are gathered the scattered prophecies of the past upon the cases in which the axe will fall. These are what properly have been called the oracles of the law. Far the most important and pretty nearly the whole meaning of every new effort of … thought is to make these prophecies more precise, and to generalize them into a thoroughly connected system.
>
> (Homes,1897: 457)

As we shall see, the computational axe has fallen many times already and will continue to fall.

This chapter examines the path of law after the computational turn. Inspired by Holmes's use of prediction to better understand the fabric of law and social change, I suggest that his predictive stance (the famous "bad man" theory) is also a useful heuristic device for understanding and evaluating the predictive technologies currently embraced by public- and private-sector institutions worldwide. I argue that today's predictive technologies threaten due process by enabling a dangerous new philosophy of preemption. My concern is that the *perception* of increased efficiency and reliability in the use of predictive technologies might be seen as the justification for a fundamental jurisprudential shift from our current *ex post facto* systems of penalties and punishments to *ex ante* preventative measures that are increasingly being adopted across various sectors of society.

This shift could fundamentally alter the path of law, significantly undermining core presumptions built into the fabric of today's retributive and restorative models of social justice, many of which would be preempted by tomorrow's actuarial justice.[6] Unlike Holmes's predictive approach, which was meant to shed light on the nature of law by shifting law's standpoint to the perspective of

[5] KDD is the acronym for knowledge discovery in databases. This field seeks to make sense of data by applying algorithms that identify patterns and extract useful knowledge from databases. See e.g. Fayyad, Piatetsky-Shapiro and Smyth (1996).

[6] The actuarial approach to criminal justice seeks to anticipate crime and 'shifts away from a concern with punishing individuals to managing aggregates of dangerous groups' (Freeley and Simon, 1992: 449).

everyday citizens who are subject to the law, preemptive approaches enabled by the computational turn will obfuscate the citizen's legal standpoint. Preemptive approaches have the potential to alter the very nature of law without justification, undermining many of our core legal presumptions and other fundamental commitments.

In the section that follows, I lay out Holmes's view of law as a business focused on the prediction and management of risk. I suggest that his famous speech, *The Path of Law,* lays a path not only for future lawyers but also for data scientists and other information professionals. I take a deeper look at Holmes's predictive theory and articulate what I take to be his central contribution—that to understand prediction, one must come to acknowledge, understand and account for the point of view from which it is made. An appreciation of Holmes's predictive stance allows for comparisons with the standpoints of today's prediction industries. I discuss these industries in section 3, where I attempt to locate potential harms generated by the prediction business associated with the computational turn. These harms are more easily grasped in section 4, where I argue that prediction, when understood in the context of risk, is readily connected to the idea of preemption. I suggest that the rapid increase in technologies of prediction and preemption go hand in hand and I warn that their broad acceptance represents a growing temptation to adopt a new philosophy of preemption, which could have a significant impact on our fundamental commitments to due process. Finally, in section 5, I conclude by reflecting on the path of law and its future in light of the computational turn.

2. HOLMES'S PREDICTIVE STANCE

Before delving into the computational turn and its implications for due process, it is worth exploring Holmes's understanding of the general role that prediction plays in law. For, as I argue below, the juxtaposition between Holmes's predictive stance and the standpoint adopted by many of today's anticipatory algorithms throws into sharp relief the risk of harm potentially generated by the computational turn.

Understanding law as a business was unquestionably one of the principal messages of Holmes' *Path of Law* speech (Gordon, 2000: 11). In particular, Holmes believes that the business of law is to predict and thereby avoid risk. The goal of Holmesian prediction is highly pragmatic: lawyers do it to keep their clients out of harm's way. For the liberal-minded Holmes, that harm generally presents itself through state coercion:

> [t]he primary rights and duties with which jurisprudence busies itself again are nothing but prophecies… a legal duty so called is nothing but a prediction that if a man does or omits certain things he will be made to suffer in this or that way by judgment of the court; and so of a legal right.
>
> (Holmes, 1897: 458)

It may be said that Holmes's predictive approach anticipates the *risk society*—what sociologist Anthony Giddens described shortly after the hundredth anniversary of the publication of *The Path of Law* as 'a society increasingly preoccupied with the future (and also with safety), which generates the notion of risk' (Giddens, 1999).

Borrowing today's terminology, one might therefore say that Holmes re-imagined law as the business of risk management. Not only did he invent the field, he also articulated its legal methodology. Although he did not use these words in *The Path of Law,* he recognized that published common law decisions could be used as the data points from which predictions about future risk avoidance could be generated. Demonstrating the instincts of today's data scientist, Holmes wondered: if prediction is the name of the game, what are the aspiring lawyers seated in this audience to do about the deluge of legal data accompanying what seemed like an exponential increase in the number of annually reported cases across the common law?

Replied Holmes,

> The number of our predictions when generalized and reduced to a system is not unmanageably large. They present themselves as a finite body of dogma which may be mastered within a reasonable time. It is a great mistake to be frightened by the ever-increasing number of reports.
>
> . . . .
>
> I wish, if I can, to lay down some first principles for the study of this body of dogma or systematized prediction […] for men who want to use it as the instrument of their business to enable them to prophesy in their turn [...].
>
> (Holmes, 1897: 474)

Could there be a better call to arms than this for the budding field of legal informatics? Even Holmes could not have predicted the fallout from remarks of this sort—in or outside of the field of law.

After all, Holmes's central aim in the speech was 'to point out and dispel a confusion between morality and law' (Holmes, 1897: 459). This, he thought, was crucial not only in a business context but also to ensure the proper study of law. Holmes hoped at the same time to expose the fallacy, 'that the only force at work in the development of the law is logic' (Holmes, 1897: 465). He wanted to replace the incumbent legal formalism and its syllogistic approach to legal education by offering a more robust and realistic method, recognizing, as he famously put it, that, '[t]he life of the law has not been logic; it has been experience. The law [...] cannot be dealt with as if it contained the axioms and corollaries of a book of mathematics' (Holmes, 1881: 1).

I think it is safe to say that Holmes's predictive approach is closely linked to his disdain of natural law theory and its confounding of law and morals. As an adherent of the tradition of legal positivism, Holmes was of the belief that legal doctrine—duties and rights, for example—are not pre-existing moral objects but social constructs that have been posited by humans in order to achieve instrumental legal purposes.

Putting the cart before the horse—confusing legal and moral ideas—Holmes thought, undermines 'a right study and mastery of the law as a business with well understood limits, a body of dogma enclosed within definite lines' (Holmes, 1897: 459). So important was this potential for confusion that Holmes constructed a perceptual device through which law could be identified and understood:

> If you want to know the law and nothing else, *you must look at it as a bad man*, who cares only for the material consequences which such *knowledge enables him to predict*, not as a good one, who finds his reasons for conduct, whether inside the law or outside of it, in the vaguer sanctions of conscience.
>
> (Holmes, 1897: 459, emphasis added)

Who exactly is this bad man and why does Holmes think *he* has a monopoly on legal understanding? In answering these questions, it is useful to remember that Holmes had already framed the business of prediction within the context of risk avoidance. Repeating his words, 'it becomes a business to find out when this danger is to be feared' (Holmes, 1897: 457). According to Holmes,

> You can see very plainly that a bad man has as much reason as a good one for wishing to avoid an encounter with the public force, and therefore you can see the practical importance of the distinction

> between morality and law. A man who cares nothing for an ethical rule which is believed and practised by his neighbors is likely nevertheless to care a good deal to avoid being made to pay money, and will want to keep out of jail if he can.
>
> (Holmes, 1897: 459)
>
> . . .
>
> But what does it mean to a bad man? Mainly, and in the first place*, a prophecy that if he does certain things he will be subjected to disagreeable consequences* by way of imprisonment or compulsory payment of money.
>
> (Holmes, 1897: 461, emphasis added)

It is worth noting that a careful reading of *The Path of Law* reveals that Holmes's bad man is perhaps *not so bad* after all. Catherine Pierce Wells describes him as 'simply someone who does not share in the ideals that the laws represent. The bad man could, for example, be a feminist, a religious fundamentalist, an abolitionist, a black separatist, a gay activist, or even a Moonie (Wells, 2000). Perhaps no one has put it better than William Twining, whose very thoughtful characterization paints the bad man as neither

> […] a revolutionary nor even a reformer out to change "the system." The Bad Man's concern is to secure his personal objectives within the existing order as painlessly as possible; he is not so much alienated from the law as he is indifferent to all aspects which do not affect him personally. […] Nor is he a subscriber to some perverse ethic which turns conventional morality upon its head. The Bad Man is amoral rather than immoral.
>
> (Twining, 1972: 280)

The implications of this 'pale, incomplete, strange, artificial man' (Twining, 1972: 280) have been enormous (see e.g. Cooter, 1998). Taking an economic perspective—seeing legal duties as disjunctive (either keep your contract or pay damages) rather than categorical (you have a duty to keep your contract)—Holmes's bad man 'eliminates the moral onus from his conduct' (Luban, 2000: 39).

Having adopted a disjunctive view of legal duty, it is therefore a defining characteristic of Holmes's bad man that he desires to predict in advance the legal outcome of his future behavior. Prediction allows him to choose a future course of action that best aligns with his own self-interest. Prediction allows him to decide whether to (dis)obey the law. It enables him to preempt unfavourable (il)legal outcomes when they are not to his advantage.

Holmes was telling a room packed full of aspiring lawyers that if they want a 'rationally motivated', 'precise' and 'predictable' understanding of what the law demands in any particular instance, they should not look at the matter from the perspective of classical analytic jurisprudence or—*got in himmel*—through the lens of morality. Instead, they should imagine themselves in their offices with 'the bad man seated across the desk […] and think of the matter from his point of view' (Luban, 2000: 37). In so doing they will realize that to investigate law from this standpoint is really just to figure out what clients need to know in order to make effective predictions regarding their future legal advantage (Twining, 1972: 286).

Here, finally, we come to what I believe is the crux of the matter for Holmes. Plain and simple: when it comes to thinking about the law, the bad man offers an important *switch in standpoint.*[7] Through the eyes of the bad man (or, for that matter, the good citizen, who is likewise concerned with legal prediction[8]), Holmes encouraged his audience to shift perspectives from the traditional narrowness of the elite classical Victorian jurist to the standpoint of everyday citizens who are subject to the law and who therefore seek to predict the future consequences of their actions. Although he did not offer a comprehensive theory of legal prediction, Holmes taught us that predictions should be understood with reference to the standpoint of everyday people, from their point of view and their sense of purpose. These important lessons are often lost in contemporary discussions of prediction, where we pay disproportionate attention to outcome-oriented features such as accuracy, reliability and efficiency.

Holmes's predictive stance is invaluable as we start to ponder the computational turn. Where Holmes left off is precisely where we should begin. As a quick recap, Holmes told us that: (i) predictions are made by lawyers; (ii) predictions are made from the point of view of the client; (iii) clients use those predictions to avoid risk of future harm through state coercion; and (iv) the prophecies of what courts will do are to be found in legal reports, treatises, and statutes and inferred by various legal methods. Extrapolating from this, when we assess some of today's predictive technologies, we ought to keep in mind the following questions: (i) who makes computational

[7] I borrow this phrase from William Twining.

[8] As Twining points out, '[t]here may also be occasions when the Good Citizen can be said to have a moral duty to predict the likely consequences of his actions. The difference between the Bad Man and the Good Citizen does not rest on the latter's indifference to prediction, but on the former's indifference to morality' (Twining, 1972: 282).

predictions?; (ii) for whom and from what perspective are computational predictions being made?; (iii) when and for what purposes?; (iv) and on what basis and by what means?

With these questions in mind, we move from Holmes's predictive theory to a more contemporary look at today's prediction industries.

3. PREDICTION INDUSTRIES

Like the Holmesian bad-man-on-steroids, we—consumers, citizens, corporations and governments in an *information society*—have come to rely on a host of computational software that can anticipate and respond to our future needs and concerns. It is instructive to briefly consider a few examples from both the private and public sectors.

I started this chapter with a reference to Google. Although we think of Google primarily as a search engine, its convergence of services is really more like a giant prediction machine. When you enter your search query, Google not only provides a list of websites related to your search terms, it also predicts which of those sites you will find the most relevant and lists them first (Google, 2010a). It does so using a search algorithm that is based upon a series of secret factors, including a proprietary technology called PageRank (Brin and Page, 2006). This ranking system generates search results from most likely to least likely, based on a series of votes.

A webpage's votes are tabulated by calculating the number of pages linked to it multiplied by its own rank value. Like other 'democratic systems', this method has its shortcomings. PageRank might assume that any vote is valid, meaning that false, fake, or misleading links apply equally.[9] As each clicked link has the potential to be someone's monetary gain, practices of cybersquatting or link renting corrupt search results (Wall, 2004). In such cases, the top hit does not accord with Larry Page's vision of the perfect search engine. Instead, the equivalent of a virtual billboard appears: an advertisement on a link that scores a high ranking on Google's search result page.

As we have seen, the *I'm Feeling Lucky* search is designed to save time by directing you straight to the page that Google predicts you were most likely looking for—the first result for your query (Google,

[9] Google is, however, constantly reworking its search algorithm in an effort to counter-act these shortcomings (Google, 2011a).

2010b). Google has extended this use of key word-based prediction beyond the search engine. Google's AdSense and AdWords programs automatically display advertisements that the technology predicts will meet your interests, based on the information you provide to various Google programs, such as Gmail (Google, 2010c) and, more recently, the social network known as Google+ (Google, 2011b). Despite its enormous fame, like many of today's anticipatory algorithms, Google is a relatively opaque technology.

Other online companies similarly use predictive advertising technologies. Take for instance Amazon's popular 'recommendations' or the iTunes Genius. Amazon's predictive algorithm considers the items that you have previously purchased, rated or told Amazon that you own and compares this information to the same information from other users. Based on what those users have purchased, Amazon will 'predict' what related items you might like and will recommend them to you (Amazon, 2011). iTunes Genius is similar. It employs an algorithm to compare the songs in your iTunes library, and information about how frequently you listen to your songs, to the same information from other iTunes users. Based on that comparison, iTunes can predict and recommend new music that you might enjoy. And of course, it gives you a direct link to the iTunes store (iTunes, 2011; Mims, 2010). Amazon and iTunes are certainly not the only online businesses using predictive algorithms to customize advertising to Internet shoppers.[10]

The social network Facebook has further expanded on these predictive data-mining techniques through its Open Graph and instant personalization technologies (Facebook Developers 2011; Facebook 2011). Instead of relying on the information that a user provides to one website, say for instance the Internet movie database IMDb, the Open Graph connects the user's online information across a host of websites by adding the user's IMDb 'likes' to her Facebook profile.[11] Facebook advertisers can then better predict the interests of that user and target advertising accordingly. The Open Graph also allows different websites that have partnered with Facebook to predict a user's preferences based on the information contained on the user's Facebook profile. A partner website can then use this

[10] For instance predictive recommendations are also popular on social network Facebook, Internet radio site Pandora.com and movie streaming site Netflix.com. See e.g. Iskold (2007).

[11] The visitor to the site may express approval for a movie by clicking a *Like* button associated that specific movie. The movie will then be added to the visitor's Facebook profile as a movie that she likes (Facebook Developers, 2010).

Facebook profile information to customize what the user sees and hears when browsing their site.[12] Open Graph can be thought of as Facebook's answer to Google Streetview—just as the relationship between physical objects on the street can be mapped by way of special cameras and software that can stitch the pieces together in a seamless whole, so too can the data points of people's personal information and preferences on Facebook be connected in ways that create a larger graphical understanding of their social landscape, allowing for a broader range of predictions to be made about individuals and groups.

Loyalty cards, matchmaking websites, and bankcard monitoring similarly try to predict habits and create customer profiles in order to determine what promotions, personal connections or cautions are applicable to specific clients.

The prediction industry is by no means limited to the private sector. Governments have many uses for predictive profiling systems as well. Perhaps the most widely known application of prediction occurs at airports and other border crossings.

For example, there are many passenger safety systems in place in airports around the world that demand additional screening from identified individuals or that prevent travelers from flying altogether. As I shall discuss further below, Canada's *Passenger Protect* program relies on predictive intelligence from the Canadian Security Intelligence Service and Royal Canadian Mounted Police to produce a computerized passenger database, which it calls the *Specified Persons List* (Transport Canada, 2009). Individuals who are deemed to pose a threat to airline security are placed in the database (Government of Canada, 2010). The system is designed to ensure that the individuals are identified before they have the opportunity to board an aircraft. The system is similar to the U.S. No-Fly List and other systems employed elsewhere (see e.g. Federal Bureau of Investigation, 2010; Transportation Security Administration, 2010).

The reliability of such algorithms has been widely decried; systems such as Soundex and CAPPS II are now defunct due to inaccuracy rates as high as 85% (Moore, 2007). Many newborn and deceased

[12] Current partner websites include search engine Bing, travel website TripAdvisor, TV recommendations website Clicker, movie review site Rotten Tomatoes, document collaboration site Docs.com, Internet radio site Pandora, restaurant review site Yelp and online reading site Scribd (Facebook, 2011).

individuals have also somehow made their way onto no-fly lists. While officials claim that listing such individuals reduces incidences of misused identity, critics claim that the bureaucracy is too slow to respond (Zetter, 2010). Memorably, Senator Ted Kennedy was briefly grounded because of confusion caused by a ‘name likeness’ with someone on the U.S. No-Fly List (Henry and Ahlers, 2004). To this day, there does not seem to be a compelling reason to have detained one of America’s most well known senators. Furthermore, reports suggest significant challenges associated with profiling terrorists; a Dutch study showed no reliable indicators that could predict which individuals are likely to embrace Islamic radicalism (Whitlock, 2007).

This brief set of descriptions and anecdotes offers a snapshot of the broad range of predictive technologies and techniques employed in the public and private sectors. Unlike legal prediction à la Holmes’s bad man, computational prediction does not adopt a singular or even uniform predictive stance. To demonstrate this point and consider some of its consequences, it is useful to return to the generalized questions extrapolated from Holmes’s work at the end of the previous section.

(i) Who makes computational predictions?

Locating the author(s) of a computational prediction is a difficult, sometimes awkward task. Prediction algorithms used by government agencies may be unavailable to the public for reasons of national security and public safety. Furthermore, many of the prediction algorithms and software applications discussed above are subject to copyright and trade secret laws, so the public does not get to know who wrote them, how they work or whether the assumptions upon which they are based are sound.[13] Difficulties in coming to know anything more about the author(s) of the prediction, let alone establishing a legal relationship with them, can be further complicated by the fact that private services are licensed to end-users for only limited purposes. To complicate matters further, locating the author(s) of a computational prediction is sometimes awkward because the creator of the algorithm or software may not in any clear sense be the author of any particular prediction generated by the system. Intelligent agent software (Kerr, 1999; Kerr, 2004) and other innovations in the field of artificial intelligence enable ‘autonomous’ computer-generated operations that are distinct from the programs

[13] This problem is not limited to the private sector. Where private companies create algorithms for government agencies, the same protections might apply (Citron, 2007).

that set them in motion and are sometimes not even fully comprehended by the human beings who did the programming. Within the context of the computational turn, predictive techniques often have no human author; sometimes there is no one who is directly accountable for any particular machine-generated prediction (Solum, 1992).

(ii) For whom and from whose perspective?

Recall that for Holmes the role and task of legal prediction is intimately and inextricably connected to the standpoint of those on whose behalf the predictions are made. The predictive stance for Holmes requires lawyers to adopt the perspective of their clients in order to promote their future interests, regardless of their moral stance. The same is untrue for most computational prediction systems. Unlike lawyers, who are bound by fiduciary duties, computational prediction providers are not usually seen as entering into personal relationships with their clients. The word *client* (which historically connotes one being under the protection and patronage of another) in this context is a misnomer. Here, the parties do not know each other. Nor does one protect the other. The so-called 'client' is in truth little more than a data subject, whose actual perspective is never considered.[14] An automated system simply collects data about the data subject and runs its algorithm(s).

Unlike lawyers or other professionals, computational prediction systems do not generate relationships of trust and therefore do not attract special duties of care in any traditional sense.[15] Rather, the duties between the parties—merely contractual in nature—are carefully circumscribed in the prediction provider's mass-market end-user licence agreement (EULA). These EULAs are typically one-sided, generally quite restrictive and often require the data subject to waive various rights to privacy and due process. Unlike the solicitor-client relationship, these EULAs ensure that the parties remain at arm's length (see e.g. the Terms and Conditions provided at iTunes, 2010). Although the services provided are often thought of as 'free', in the sense that they do not cost money, the personal information

[14] Except perhaps from the standpoint of some social category to which they are presumed to belong, whether or not they actually belong (Hildebrandt and Gutwirth, 2008).

[15] Elsewhere I have argued that we ought to consider online service providers as fiduciaries when they are the stewards of our personal information (Kerr, 2001).

that is collected and used in exchange for the prediction service is often so valuable that it is the basis of the entire business model.[16]

In many cases, the prediction service is little more than an appendage to a broader range of sales and services provided, none of which involve taking into account the standpoint or future interests of the data subject. At best, there is a willingness to stroke certain consumer preferences in exchange for valuable personal information, the implications of which are usually obfuscated and unclear from the actual perspective of the data subject. For example, the predictive recommendations made by Amazon or iTunes are less about serving clients than they are about mining data about individual preferences in order to sell stuff. Unlike legal or medical predictions, which aim to benefit the well being of the client or patient,[17] much of today's private sector prediction industries serve a broader corporate mandate that seeks first and foremost to benefit the information service provider.

Of course, the situation is even worse for computational systems designed to render predictions *about* data subjects. In contrast to Holmesian legal prediction, the entire basis of which was to shield citizens from the threat of state sanction, modern social sorting and profiling techniques such as no-fly lists are designed to promote corporate and state interests such as profit, prosperity, security and safety, often at the expense of any given citizen. As part of a broader adversarial system, technologies of this sort are meant to generate predictions entirely at odds with the interests of the data subjects, especially when they are presumed to be the 'bad man.' It is important to note that, unlike Holmesian prediction, these are *not* predictions about legal outcomes. For the most part, they are behavioural predictions about the supposed future conduct of individuals, often based on their past behaviour or their associations with other individuals and groups (Wilson and Weber, 2008; McCulloch and Pickering, 2009).

[16] It is valuable not only to other private sector partners but to public sector entities, who will pay vast sums for it in order to build databases for their own KDD applications. KDD in government and industrial applications is specifically geared towards enabling better decision-making or better delivery of services. This can permit governments to make decisions based on scientific or statistical support. See Shu-xiao et al (2006).

[17] For example, diagnosis decision support software allows physicians to enter a patient's symptoms into the program and the software will 'predict' and display potential diagnoses (see e.g. Isabel Health Care, 2011; Nolo, 2010).

(iii) When and for what purposes?

Predictions are by definition anticipatory. To predict is to say or know something before it happens.[18] As we saw with Holmes, legal prediction allows a lawyer to anticipate the consequences of future courses of conduct in order to advise clients whether it is feasible or desirable to avoid the risk of state sanction. I will call predictions that attempt to anticipate the likely consequences of one's action, *consequential predictions.*

With this definition, one sees right away that many of the predictive technologies discussed above are of a different sort. When I ask iTunes Genius to anticipate which songs I will like, the system is not generating predictions about my conduct or its likely consequences. Rather, it is trying to stroke my preferences in order to sell me stuff. Much of the prediction business is focused on predictions of this sort, which I shall refer to as *preferential predictions.* Like the lawyer's consequential predictions, preferential predictions are meant to increase a person's future options, but in a more materialistic way and usually from the perspective of the vendor.

There is a third form of prediction exemplified by a number of the technologies that form part of today's prediction industries. Unlike consequential and preferential predictions, *preemptive predictions* are used to diminish a person's future options. Preemptive predictions assess the likely consequences of (dis)allowing a person to act in a certain way. Immediately, one should recognize that these predictions do not usually adopt the perspective of the actor. Preemptive predictions are mostly made from the standpoint of the state, a corporation or anyone who wishes to prevent or forestall certain types of action. Preemptive predictions do not assess an individual's actions but whether the individual should be permitted to act in a certain way. Examples of preemptive prediction techniques include a no-fly list used to preclude possible terrorist activity on an airplane, or a regionally coded DVD that automatically scrambles the North American display of movies bought in Europe (thus preempting presumed copyright infringement).

These three categories of prediction—consequential, preferential and preemptive—are not meant to provide an exhaustive list of all possible predictive purposes. But, as I will articulate in the sections that follow, understanding these different predictive purposes will

[18] *The Oxford English Dictionary*, 2d ed, *sub verbo* 'prediction'.

help to locate the potential harm of various predictive technologies associated with the computational turn.

(iv) On what basis and by what means?

The question ‘on what basis and by what means are computational predictions made?’ is, for the most part, best left to the chapters in this volume written by data scientists. Not only because of the technical nature of the answers to such questions but also because of how little is publicly known about the means by which some of the more significant examples of computational predictions are made. As mentioned above, it is important to recognize that the basis and means by which particular predictions are generated are often developed in a context where secrecy is tantamount to the success or profitability of the product. I challenge any technologist in the world not involved in the development or maintainance of such systems to publicly detail *exactly* how Google’s secret algorithm works or how the U.S. Terrorist Screening Center’s No-Fly List is computed.[19]

At the end of the day, the attempt to provide even basic answers to this question (‘on what basis and by what means?’) and the three questions that preceded it leads me to end this section of the inquiry with a circumlocution of Holmes’s great opening line in *The Path of Law:*[20] When we study predictive algorithms we are studying a mystery, *not* a well-known profession.

4. PREDICTION AND PREEMPTION

The power of today’s predictive techniques and their potential for harm are perhaps best understood in the context of risk. In Section 2, I mentioned that Holmes’s predictive approach anticipates the *risk society.* When sociologist Ulrich Beck coined this term in the 1990s, he was not suggesting that society is more risky or dangerous nowadays than it was before. Instead, he set out to describe the manner and extent to which modern society is organized in response to risk.

[19] Google has consistently rejected calls to make its search algorithm public or to implement ‘neutral search’ rules that would be regulated by a government or other oversight body (Mayer, 2010).

[20] “When we study law we are not studying a mystery but a well-known profession.”

Beck believes that, in modern society, 'the social production of wealth is systematically accompanied by the social production of risks' and that, accordingly,

> the problems and conflicts relating to distribution in a society of scarcity overlap with the problems and conflicts that arise from the production, definition and distribution of techno-scientifically produced risks.
>
> (Beck, 1992: 19)

On Beck's account, risk and prediction are interrelated concepts. He subsequently defined risk as 'the modern approach to foresee and control the future consequences of human action'—which he believed to be the 'unintended consequences of radicalized modernization' (Beck, 1999: 3).

Holmes saw this connection as well, contending that prediction is a means of avoiding risk. Much like Beck, Holmes had also recognized that the production of risk is lucrative. It is therefore no surprise that Holmes used the legal device of contract to illustrate both prediction and risk as valuable commodities. When we create a contract, we obtain benefits in exchange for undertakings; we get something now with a probability of being forced to pay for it later. In other words, we create risk—we mortgage our future selves in favour of our present selves. Legal prediction is a highly valued commodity for clients who seek to avoid or mitigate future legal risk. At the same time, the production of legal risk (e.g., the creation of a contract or the assumption of debt) is invaluable to both lawyers and their clients.

Taken together, Holmes and Beck help to demonstrate the clear connection between risk and prediction. To put it bluntly, prediction industries flourish in a society that is organized in response to risk. This is because prediction often precipitates the attempt to preempt risk.

The relationship between prediction and preemption was of less import to Holmesian society than it is to the risk society. Holmes's preoccupation was the power of the state over individuals, which generated an interest in what I have called consequential predictions: predictions about the likely (legal) consequences of the bad man's actions.

By contrast, in a society that is organized in response to risk—where *anyone* can be the bad man—there is a heightened interest in preemptive predictions: predictions that assess the likely consequences of (dis)allowing a person to act in a certain way. Given the above analysis regarding the relationship between risk and prediction, it stands to reason that the escalating interest in (preemptive) predictions will provide the justification for new forms of social preemption. In much the same way that Holmesian clients use legal prediction to preempt future legal risk, governments, corporations and individuals will use predictive technologies in order to preempt or forestall conduct that is perceived to generate social risk.

The *Specified Persons List* mentioned in Section 3 provides an illustration. With an increased (perception in the) ability of government agencies to successfully predict which individuals will pose a threat to national security, this deeply controversial list[21] catalogs an inventory of individuals who are preempted from boarding a commercial aircraft for travel in or out of the country. Canada's *Passenger Protect* system, implemented in 2007, preempts from flight anyone on the *Specified Persons List*, i.e*.,* anyone 'who may pose an immediate threat to air security' (Government of Canada, 2010). The means of predicting who poses a risk sufficient to preempt them from flying includes a (partially) computer-generated assessment of,

> - past history with regards to acts of violence, terrorism, criminal acts and/or convictions, active association with known or suspected terrorists and/or terrorist groups and their personal history of terrorist acts;
> - the individual's intent with regards to engaging in a hostile act that may involve or threaten transportation or aviation; and
> - the individual's capability based on their knowledge, abilities and/or experience, which may be used to threaten or harm aviation or transportation.
>
> (Government of Canada, 2010)

Prior to the development of this list, those perceived to be high-risk individuals were still free to travel—unless there were reasonable and probable grounds to believe that the high risk individual was actually in the process of committing an offence. A no-fly list preempts the need for any such evidence. In the risk society, prediction replaces the need for proof.

[21] As one commentator has put it, the enumerated individuals are somehow so dangerous that they are not allowed to fly, yet so innocent that they are permitted to roam Canadian streets freely (Kutty, 2007).

Though nascent, the private sector also has a deep interest in the development and use of preemptive technologies. A typical example is the growing use of digital locks to preempt unauthorized individuals (read: high risk hacker-types) from accessing copyrighted works. Prior to the development of these digital technologies, the entire system of copyright was premised on the notion that individuals are free to consume intellectual works and free to copy and share them within the limits of copyright law—without ever asking for anyone's prior permission to do so. Under the old system, copyright owners also had the right to sue anyone that they believed to be infringing their copyright. But they *did not* have the legal right or technological power to preempt access to the work altogether. Now they have both. First, they have the technological capability to wrap digital locks around digital content so that only those with prior authorization can access it (Stefik,1997; Stefik, 1996). Second, in many jurisdictions, this form of technological preemption is in fact state sanctioned. Not only is preemption legally permitted, in many countries there are laws that prohibit tampering with the digital lock—even if the lock-breaker has proprietary reasons for doing so and never intended to infringe copyright in the process (Kerr, 2010; Kerr, 2005). This state sanctioned preemption of access to digital content has a tremendous impact on various rights and freedoms, including: access to information, freedom of expression, privacy, encryption research, freedom to tinker, education, as well as copyright's delicate balance between owner and user rights.

Of course, similar preemptive techniques can be employed beyond the copyright sector. They can be used to prevent a broad range of activities limited only by the technological imagination, from drinking and driving (O'Donnell, 2006) to filtering out sounds that are not part of the prepaid bundle of services subscribed to by a patient with cochlear implants (Kerr, 2011).

It is tempting to view the broad adoption of the above technologies in both the public and private sector as evidence of a potential shift towards a new philosophy of preemption—what two authors recently styled the 'duty to prevent' (Feinstein and Slaughter, 2004). Perhaps the best illustration of this philosophical shift is the legal and technological approach to counter-terrorism, exemplified by what has become known in international law as the 'Bush Doctrine'.

President Bush first publically discussed preemption in a speech at West Point on June 1, 2002:

> If we wait for threats to fully materialize, we will have waited too long. … We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge...our security will require all Americans to be forward-looking and resolute, to be ready for preemptive action when necessary to defend our liberty and to defend our lives.
>
> (United States Military Academy, 2002)

Those who subscribe to the philosophy of preemption believe that '[p]erpetrators of terrorist attacks now operate from a dispersed and invisible transnational network—terrorists are "here, there and everywhere"' (Nabati, 2003: 779).[22] Here, the terrorist is the ubiquitous bad man. Whereas the word 'criminal' connotes a person who has committed a crime at some point in the past, the future threat of the terrorist looms large. In other words, the terrorist concept is inherently preemptive,

> Countering terrorism is uniquely suited to a shift to pre-crime frameworks because the term 'terrorism' itself is pre-emptive, existing prior to and beyond any formal verdict.
>
> (McCulloch and Pickering, 2009: 630)

McCulloch and Pickering's reference to pre-crime frameworks is of course an allusion to Philip K. Dick's famous 1956 short story, *The Minority Report* (Dick, 1956). Dick imagines a future society that has fully embraced the philosophy of preemption. The preemption of crime is made possible through the technological mediation of three mutant precogs who, together, form a prediction machine able to forecast future outcomes with stunning accuracy and reliability. Blurring the lines between deterrence and punishment, the pre-crime system preemptively incarcerates individuals whenever the precogs predict that they will commit a future crime. This predictive system replaces the traditional criminal justice system of discovering a crime and its perpetrator *ex post facto*, presuming the accused's innocence, then, through due process, establishing guilt and, finally, issuing an appropriate punishment. Like the no-fly list, we see that prediction replaces the need for proof.

Whether Dick was himself predicting the future or providing its blueprints by way of a self-fulfilling prophecy, modern data-mining techniques are already being used to carry forward this preemption philosophy (Steinbock, 2005; Beecher-Monas, 2003). For example,

[22] Or, as the then U.S. Secretary of Defense, Donald Rumsfeld, put it, 'We know where they are. They're in the area around Tikrit and Baghdad and east, west, south and north somewhat' (United States, 2005: 25716).

Richard Berk, Professor of Statistics and Criminology at the Wharton School, University of Pennsylvania, (University of Pennsylvania, 2011) has developed an anticipatory algorithm that sifts through a database of thousands of crimes and uses algorithms and different variables, such as geographical location, criminal records and ages of previous offenders, to come up with predictions of where, when, and how a crime could possibly be committed and by whom (Watson, 2010). Versions of this technology have already been adopted in Baltimore and Philadelphia to predict which individuals on probation or parole are most likely to murder and to be murdered (Bland, 2010). Washington D.C. has recently implemented a newer version of the software, which will identify individuals most likely to commit crimes other than murder.

Although the 'precrime' concept is not directly at play, Professor Berk's anticipatory software is already being used to help determine how much supervision parolees should have based on predictions about how they are likely to behave in the future. Professor Berk says the program will also play an invaluable role in future determinations for bail and sentencing hearings (Bland, 2010). For better or for worse, his software, which merely computes statistical probabilities, is already preempting the life chances and social opportunities of thousands of data subjects across various jurisdictions in a very real way. And Professor Berk's software is not the only game in town—there are a growing number of similar systems in use throughout the United States and the United Kingdom.[23]

Reports such as these are often exaggerated and even more often used to prophesize the coming era of the *Minority Report,* and the idea that we are 'sleepwalking into a surveillance society.'[24] This is not my purpose. The more modest claim that I have tried to articulate in this section is that prediction, when understood in the context of risk, is easily connected to the idea of preemption. If this is correct, it should therefore come as no surprise that technologies of prediction

[23] Such as Memphis Police Department's use of IBM's new Blue CRUSH (Crime Reduction Utilizing Statistical History), an analytics software system that predicts trends, allocates resources and identifies "hot spots" to reduce crime rates (SPSS, 2011 – note to editor: use date of access?). Researchers from Queen's University Belfast have added CCTV cameras to the equation, using ISIS (Integrated Sensor Information System) computer vision technology in order to 'profile individuals to see if they pose a risk and then to check for patterns of behaviour that may be suspicious or anti-social' (Centre for Secure Information Technologies, 2011; Alleyne, 2009).

[24] This idea was raised by British Information Commissioner, Richard Thomas, when expressing his concern about government proposals for national identification cards and population databases (Ford, 2004).

and preemption go hand-in-hand. Not because they are somehow inevitably linked but simply because, as Holmes told his audience so long ago, 'people want to know under what circumstances and how far they will run the risk of coming against what is so much stronger than themselves, and […] to find out when this danger is to be feared' (Holmes, 1897: 457).

A careless and excessive adoption of the preemption doctrine could have a significant impact on our fundamental commitments to justice and due process, unraveling many core presumptions that stitch together the very fabric of our legal system. In section 5, I highlight a few key threads and show how they might be unknotted by today's predictive and preemptive techniques.

5. HOW PREDICTION AND PREEMPTION UNDERMINE DUE PROCESS

The coupling of preemptive goals with predictive techniques, discussed in the previous section, signals an important concern shared by many who study the relationship between law and technology. Technologists have the ability to impose upon the world norms of their own making—promulgated not through democratically enacted legal code but through the oligarchy of software code (Reidenberg, 1998; Lessig, 2006). Left unchecked, predictive and preemptive technologies provide tremendous power to programmers and those who utilize their technologies. They are able to use software to regulate human behavior and make key decisions about people without the usual legal checks and balances furnished in real space. Artificial intelligence pioneer, Joseph Weizenbaum, was not kidding when he once said that, '[t]he computer programmer is a creator of universes for which he alone is responsible. Universes of virtually unlimited complexity can be created in the form of computer programs' (Weizenbaum, 1976). From a broad legal and ethical perspective, problems are sure to arise when anticipatory algorithms and other computational systems import norms that undermine the due process otherwise afforded to citizens by law (Hildebrandt, 2008). In the final two sections of this chapter, I consider—à la Weizenbaum—whether predictive programs have the potential to re-write the code of the legal universe by re-programming some of its core normative presumptions.

If the legal universe has a 'prime directive' (Joseph, 1975), it is probably the shared understanding that everyone is presumed innocent until proven guilty. This well-known legal presumption is usually construed, narrowly, as a procedural safeguard enshrined in criminal and constitutional law (Quintard-Morenas, 2010; Schwikkard, 1998). However, it can also be understood as a broader moral claim, the aim of which is to provide fair and equal treatment to all by setting boundaries around the kinds of assumptions that can and cannot be made about individuals. These boundaries are intended to prevent certain forms of unwarranted social exclusion (Gandy, 1993; Ericson, 1994).

In the context of criminal procedure and administrative law, the systematic safeguards underlying this broader understanding of the presumption of innocence generally include: timely and informative notice of a hearing; an ability to know the case against you; a fair and impartial hearing; an opportunity to respond; an ability to question those seeking to make a case against you; access to legal counsel; a public record of the proceedings; public attendance; published reasons for the decision; and, in some cases, an ability to appeal the decision or seek judicial review (Friendly, 1974-1975). Although European tradition historically labeled these rights under the heading of 'equality of arms' (Wasek-Wiaderek, 2000), many common law and civil law jurisdictions now refer to this bundle of normative legal rights and presumptions as 'due process' (Shipley, 2008).

Due process is primarily understood as a creature of public law. However, much of the private sector is imbued with a corollary set of presumptions and safeguards with similar aims and ambitions. Indeed, there are many parallels between the duties owed by the state to its citizens and the duties owed by corporations to employees and customers.[25] A host of legal and ethical norms in the private sector mirror due process guarantees in public law. These are usually expressed in the form of: a right to full information; a right to be heard; a right to ask questions and receive answers; and a right of redress. Basic rules of fairness such as these are often adopted or otherwise imposed upon the private sector—even where criminal and constitutional due process rights are not in play.

[25] Corporations may owe legal duties to customers and employees, as elaborated below with respect to data protection legislation, or they may owe a normative duty to treat customers and employees fairly lest they develop a bad business reputation or lose customers (see e.g. Donoghue and de Klerk, 2009; Gilliland, 1995).

For example, in the North American workplace, prospective employees—even if never hired—are entitled to fair treatment during the recruiting process.[26] Among other things, this means that in order to ensure that job applicants perceive the hiring process as fair, employers need to offer interviewees an opportunity to: demonstrate their knowledge and skill; be evaluated only on relevant skills; ask questions about the selection process; receive timely and informative feedback on the decision-making process; challenge its outcomes; etc. (Gilliland, 1995). Because hiring is among the most fundamental of decisions made about a person in our society, something like due process is required to ensure that people are treated fairly. Principles of this sort are meant to provide job applicants with the opportunity to participate and be heard, ensuring that hiring decisions are not made on the basis of faulty predictions or presumptions, so that no one is unfairly preempted from employment.

A second example occurs in private sector data protection practices implemented throughout Europe, Canada and in various sectoral laws in the U.S. (FTC, 2007). Originally promulgated as guidelines by the OECD (OECD, 1980), most of these laws are also founded on basic principles of fairness—sometimes known as 'fair information practice principles'. In much the same way that due process requires notice prior to a trial or administrative hearing, fair information practice principles require data subjects to be notified about information sharing practices[27] prior to decisions about the collection or disclosure of their personal information. With the aim of achieving 'informational self-determination' (Federal Constitutional Court of Germany, 1983; German Data Forum, 2010: 632-633), data subjects are provided timely and affordable means of access to data collected about them and are likewise permitted to contest its accuracy (FTC, 2007). Where self-regulatory models fall short, data subjects are usually entitled to various means of enforcement and redress—including private rights of action enforced by courts or administrative bodies (FTC, 2007).

[26] Job applicants may have legal entitlements to fair treatment (for instance, human rights legislation can prohibit certain criteria from being considered in the hiring process, see e.g. Ontario's *Human Rights Code*, R.S.O. 1990, c. H. 19 s. 5(1)) as well as normative entitlements to fair treatment (Gilliland, 1995).

[27] Not merely pertaining to whom the information will be shared but, also, the uses to which the data will be put, the steps taken by the data collector to ensure confidentiality, security, integrity and the quality of the data (see e.g. OECD, 1980: Part II; PIPEDA, 2000)

A number of broader due process values underlie the data protection model, including: openness, accountability, consent, accuracy of information, and reasonable limits on collection and use (*Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5: Schedule 1). Among other things, the embedding of these values into the data protection model seeks to ensure that information will not be used out of context to make unwarranted presumptions or predictions that could unfairly implicate the life chances or opportunities of data subjects (Nissenbaum, 2009). More and more, private sector entities are being called upon to develop due process-friendly procedures aimed at ensuring fairness to individuals about whom personal information is collected, used or disclosed. This has resulted in the adoption of similar due process guidelines by the United Nations and throughout Europe and North America for a broader range of consumer protection issues (see e.g. United Nations, 2003; European Commission, 2005; *Consumer Protection Act*, S.O. 2002, c. 30, sch. A. (Ontario); Massachusetts Office of Consumer Affairs and Business Regulation, 2011). Some academics have further argued that we need a special regime to extend due process requirements to systems operators on the Internet, recognizing that the actions of system operators 'can become the occasion for substantial injustice if […] imposed without adequate cause or without the use of procedures that give the user (and, perhaps, the cybercommunity) a chance to be heard' (Johnson, 1996).

At its core—whether in the public or private sector, online or off—the due process concept requires that individuals have an ability to observe, understand, participate in and respond to important decisions or actions that implicate them.

Of course, these rights are precisely what some predictive and preemptive technologies seek to circumvent. To take one recent example, the State of Colorado recently implemented a Benefits Management System (CBMS) that uses predictive algorithms to automate decisions about an individual's entitlement to Medicaid, food stamps and welfare compensation (Citron, 2007-2008: 1256)**.** Historically, important decisions of this sort were administrative decisions subject to due process. But this is no longer so. In fact, the entire point of automated systems such as CBMS is to streamline or eliminate administrative process in order to maximize efficiency and reduce transaction costs (Hammons and Reinertson, 2004). Used with increasing frequency by governments and the private sector, such systems minimize or in many cases remove human beings from the decision-making process altogether – not just the human decision-makers but also the subjects of these decisions. This becomes deeply problematic when automated systems go awry, as was the case with the CBMS. Owing to hundreds of programming errors in the translation of the State’s benefits rules into computer code, CBMS issued hundreds of thousands of erroneous Medicaid, food stamps and welfare eligibility decisions, negatively affecting the lives of an even greater number of people than would have been affected by a slower, human-run system (Smith, 2006; Booth, 2011).

In her extremely thoughtful article on ‘Technological Due Process’, Professor Danielle Citron very convincingly demonstrates the dangers of such predictive and preemptive technologies: they undermine notice requirements, obfuscate the right to be heard and thwart participation and transparency in a rapidly eroding public rule-making process (Citron, 2007-2008). Professor Citron provides some well-tailored solutions, advocating a new model of technological due process. Drawing on the rules-versus-standards literature in U.S. administrative law, she offers surrogate rules to prevent errors and increase transparency, accountability and fairness. She also considers new standards that might be encoded into the software to prevent arbitrary decision-making. Her overarching aim is to find a means of protecting due process, ‘without forgoing the benefits offered by computerized decision systems’ (Citron, 2007-2008: 1313).

Embedding pragmatic solutions into the architecture of new and emerging technologies on a case-by-case basis is a popular approach in the privacy field (Information and Privacy Commissioner of Ontario, 2011). But what of the potentially deep systemic problems sure to arise as we scuttle the justice system in favour of efficient actuarial models, as we shift away from law’s foundational commitment to righting wrongs, opting instead for the adoption of technological systems that prevent and preclude them? Are there not reasonable limits to the kinds of things that institutions should be allowed to presume and predict about people without their involvement or participation? To what extent and by what means should institutions be permitted to organize in relation to such presumptions and predictions?

6. THE PATH OF LAW AFTER THE COMPUTATIONAL TURN

Contemplating these difficult questions, it is useful to return one last time to Holmes's approach to legal prediction. Recall that one of Holmes's most important contributions to jurisprudence was his recognition that *point of view* matters. Understanding law from the point of view of the bad man or his lawyer—who seek nothing other than accurate predictions about what courts will do in fact—is *in fact* an endorsement of due process.[28] After all, it is not possible for legal subjects or their counsel to make predictions about what courts or tribunals will do without the ability to observe, understand, participate in and respond to the decision-making process. Due process is a prerequisite of legal prediction. Yet, due process is precisely what is thwarted when the predictive focal point shifts from the law's rules and decisions to its subjects.

As discussed in Section 3, the computational turn has not only improved our ability to make consequential predictions about what courts will do, it has also vastly expanded the capability for producing preferential and preemptive predictions about people. Such predictions are now used routinely by institutions with financial or security related interests for social sorting and actuarial decision-making. Holmes's original vision of human beings making predictions about institutions for individual benefit has rapidly given way to a very different model: machines making predictions about individuals for the benefit of institutions. Except in the most perverse sense, this is no longer a client- or citizen-centric approach.

In either case, if one essential element of any just decision-making process is its predictability, then it must be possible for the subjects of those predictions—whose life chances and opportunities are in the balance—to scrutinize and contest the projections and other categorical assumptions at play within the decision-making processes themselves. While this should by now be an obvious point in the context of law courts and regulatory tribunals, as I suggested in the previous section, similar considerations apply in a number of private sector settings. Such considerations will become increasingly significant in both public and private sector settings, especially in light of our emerging understanding that, '[t]he application of probability and statistics to an ever-widening number of life-decisions serves to reproduce, reinforce, and widen disparities in the

[28] I owe this brilliant insight to the wonderful Mireille Hildebrandt.

quality of life that different groups of people can enjoy' (Gandy, 2009; see also Hildebrandt, 2010).

The threats to due process posed by the computational turn should therefore cause grave concern not only to Holmes's bad man, but also to everyone else seeking to avoid unfair treatment in public and private decision-making. Unfortunately, Holmesian positivism offers little in the way of protection. Having bathed the law in 'cynical acid' (Holmes, 1897: 462), cleansing it of any and all moral stain, Holmes undermines any normative basis of complaint for citizens who wish to ensure predictability and fairness in decisions being made about them.

This did not go unnoticed by subsequent jurists. Lon Fuller, for example, sought a corrective through the refinement of eight fundamental 'principles of legality' required to ensure predictability and fairness in the bumbling decisions of an imaginary lawmaker named *Rex* (Fuller, 1964: 33). According to Fuller's famous postulation, legal rules and decision-making systems must be: (i) sufficiently general; (ii) publicly promulgated; (iii) sufficiently prospective; (iv) clear and intelligible; (v) free of contradiction; (vi) sufficiently consistent over time; (vii) not impossible to comply with; and (viii) administered so that individuals can abide by them (Fuller, 1964: 39). For Fuller, these due process-type principles are absolutely foundational. As he put it,

> A total failure in any one of these eight directions does not simply result in a bad system of law; it results in something that is not properly called a legal system at all, except perhaps in the Pickwickian sense in which a void contract can still be said to be one kind of contract
>
> (Fuller, 1964: 39).

Some commentators have questioned whether these eight principles provide an 'inner morality' of law, as Fuller contended (see e.g. Dworkin, 1965; Kramer, 1998; Hart, 1958). Other jurists have addressed the more specific question of whether Fuller's principles demonstrate a necessary connection between law and morality, *contra* Holmes's separability thesis (Simmonds, 2007). These important philosophical questions notwithstanding, perhaps the more appropriate reading of Fuller in the present context—one that Holmes surely could have lived with—is simply that Fuller reinforces predictability as an essential legal attribute, postulating a number of necessary preconditions for the possibility of predictability and fairness in law and in life. Even the bad man needs King *Rex* to promulgate and adhere to basic due process principles in order to secure personal objectives and avoid risk within the existing legal order.

When considering the future path of law, it is crucial to see that the computational turn threatens the bad man (and everyone else) in this very respect. The computational turn provokes various questions about whether our jurisprudential aspirations of predictability and fairness remain viable in the face of a generalized institutional adoption of anticipatory algorithms and other actuarial approaches of the sort discussed in this chapter. Or, to use Fuller's parlance instead, whether a broad uptake of predictive and preemptive approaches across the social order might reach a tipping point wherein our systems of social control could no longer properly be called a 'legal system'.

I have suggested that an increasing institutional use of predictive and preemptive technologies facilitates the first steps away from our current *ex post facto* systems of penalties and punishments towards a system that focuses on *ex ante* preventative measures. If this approach were to be generalized across various key institutions, it would threaten core rights and presumptions essential to our retributive and restorative models of social justice. Indeed, a shift of this nature could quite plausibly risk a 'total failure' of several of Fuller's eight principles of legality. It would likewise sabotage Holmesian prediction. Recall one last time that Holmes believed that predictions should be understood with reference to the standpoint of everyday people, made from their point of view and operationalized with their sense of purpose in mind. This important insight has been eclipsed by today's outcome-oriented prediction industries, which tend to use people as mere means to their institutional ends. Although accuracy, reliability, efficiency and the bottom line are laudable social goals, this approach ignores the insight underlying the presumption of innocence and associated due process values—namely, that there is wisdom in setting boundaries around the kinds of assumptions that can and cannot be made about people.

Given the foundational role that due process values play in our legal system, a lingering question is therefore whether law ought to set reasonable limits on the types of presumptions and predictions that institutions are permitted to make about people without their involvement or participation. And, if so, how? Though questions of system design will continue to be important in promoting technological due process, it is no substitute for addressing important threshold questions about the broader permissibility of prediction, preemption and presumption in the face of the computational turn. I hope that this chapter inspires further research in this regard.