5.1 Introduction: The Lure and Confusion of Governmental Data Mining

Governments are facing new and serious risks when striving to assure the security and safety of their citizens. Perhaps the greatest concern is the fear of terrorist attacks. Various technological tools are being used or considered as means to meet such challenges and curb these risks. Of the tools discussed in the political and legal sphere, data mining applications for the analysis of personal information have probably generated the greatest interest. The discovery of distinct behavior patterns linking several of the 9/11 terrorists to each other and other known operatives has led many to ask: What if data mining had been applied in advance? Could the attacks and their devastating outcomes have been avoided?

Data mining has captured the imagination as a tool which can potentially close the intelligence gap constantly deepening between governments and their new targets—individuals posing a risk to security and the public’s well-being (Jonas and Harper 2006; Schneier 2006).¹ Data mining is also generating interest in other governmental contexts, such as law enforcement and policing. In recent years, law enforcement has shifted to “Intelligence Led Policing (“ILP”; Cate 2008). Rather than merely reacting to events and investigating them, law enforcement is trying to preempt crime. It does so by gathering intelligence, which includes personal information, closely analyzing it, and allocating police resources accordingly—all tasks which could be enhanced by data mining technology (IBM 2010).² The growing appeal of data mining in all these contexts results from similar reasons—the development of cutting edge technologies, advances in mathematics,

² For a paper discussing these initiatives in the Netherlands, see van der Veer et al. (2009).
statistics, and computer science, and the sinking costs of the hardware, software, and manpower needed for their implementation (Zarsky 2002–2003). The reports on the success of data mining in predicting human behavior (Ayres 2007; Baker 2008) in the commercial realm have also strengthened these models’ appeal.

It thus should come as no surprise, that in the United States, data mining initiatives are popping up everywhere. A recent GAO report indicates current data mining initiatives in a broad array of contexts (U.S. General Accounting Office 2004). DARPA has famously promoted the Total (later changed to “Terrorist”) Information Awareness (“TIA”) Program—an ambitious project which planned to analyze vast amounts of personal information from governmental and commercial sources. This project was catastrophically handled in terms of public relations. Public concerns and outrage led to Congressional intervention and the project’s quick demise (Cate 2008, 441). However, it is broadly understood that similar projects are living on, under different names and acronyms.

The reaction to the data mining of personal information by governmental entities came to life in a flurry of reports, discussions, and academic papers. The general notion in these sources, as well as the one in the public sphere is that of fear and even awe. Information privacy, which many feel is under constant attack in both the commercial and governmental realm, seems to be utterly compromised. Many share the visceral feeling that the outcome of data mining analyses, which enable the government to differentiate among individuals and groups in novel ways, is extremely problematic. The quick demise of the TIA program serves as a case in point.

Understanding what stands behind this strong visceral response is a difficult task. Even though governmental data mining is extensively discussed in recent literature (Cate 2008; Ramasastry 2004; Slobogin 2008; Solove 2008), an overall sense of confusion is ever present. Given the fact that data mining will probably prove necessary (or a “necessary evil” for some) scholars have moved to examine whether the problems it generates could be mitigated and how its risks and benefits should be balanced. While mapping out these matters, scholars as well as policy makers will be required to further establish which paradigms of legal thought are most fitting to address these matters. For that, they will examine constitutional law, privacy law, anti-discrimination law, and other matters. Yet as this discourse unfolds, something is still missing. An important, yet often overlooked, methodological step must be part of the inquiry mentioned above—the adequate consideration of alternatives. Scholars and policy makers swiftly point out the troubles of data mining as well as the dangers of ignoring it. Yet they are not equally quick to consider the detriments and shortcomings of alternatives which will surely be applied by governments setting data mining aside. Understanding the importance of this analytical step follows

4 Such success has been recently detailed in several popular books—see Baker (2008).
5 This outcome is interesting, as stories related to privacy in general have generated limited interest, less they involve an actual catastrophe—personal data about a judge blocks his nomination, information regarding the address of an actress leads to her murder, and many other examples. Yet the data mining stories here addressed focus on potential harms, which have yet to materialize. This outcome tells an interesting story about the risks of data mining.
from acknowledging that the challenges bringing data mining to the forefront of our discussion are not going away. Governments must address new security and law enforcement challenges and pressure to take action. They must also face the challenges of optimally utilizing the vast volumes of personal information at their disposal. Considering alternatives is also helpful in sharpening our understanding of the benefits, determinants, traits and qualities of data mining itself.

This chapter strives to bring the methodology of examining alternatives to the attention of academics and policy makers. It provides basic tools for engaging in this important analytic exercise. To do so, the chapter proceeds as follows: In this section, it briefly demonstrates and defines what the governmental data mining initiatives are. This is a crucial step, as the term “data mining” has almost taken on a life of its own, and is applied in several, at times contradictory, ways. The chapter also notes specific unique traits of these practices, while focusing on the distinct roles of humans and machines. These will prove constructive later, when striving to understand how it differs from its alternatives. The next Sect. 5.2 maps out, with a very broad brush, the various concerns data mining generates while drawing from the ongoing literature regarding this issue. The last Sect. 5.3 introduces four alternative strategies of personal data usage and management (or lack thereof) for achieving the governmental objectives of security and law enforcement. It also addresses an additional strategy (contemplated by policy makers and think tanks) for using a specific form of data mining while anonymizing the data. In the second segment of this section, I sharpen the distinctions between the central alternatives, so to promote a better understanding of their advantages and shortcomings.

The discussion of data mining and its alternatives goes beyond the actions of government. Private entities are using similar techniques to distinguish among their actual or prospective clients/customers, while analyzing personal behavior. These practices are applied by advertisers, marketers, management and in even more questionable settings, banks credit card issuers and insurance companies (Scism and Maremont 2011). While this context is important, it is beyond our current scope. It should be noted, however, that the rationales and internal balances discussed in the governmental context cannot be applied directly to the private sector. With private firms, competitive forces (when these indeed exist) might play an important role in achieving some of the needed objectives. However, these differences and their implications must be explored elsewhere.

Finally, although the paper claims to merely make a methodological contribution, I confess to arguing a normative point between the lines. While I do not carry through a full analysis of the pros and cons of the data mining strategies, my sense is that when taking the full scope of alternatives into account, data mining is far less problematic than when considered at first blush. The problems data mining brings to mind persist,

---

6 In some instances, the services rendered are not essential, thus allowing for consumer choice—an option which requires rethinking many of the elements to be addressed below. Finally, the obligations and motivations of governmental entities are different than their commercial counterparts, thus altering the internal calculus leading to the final recommendations.
and with greater force, when applying other options. Understanding this point might lead policy makers to reconsider the overall negative treatment data mining options receive in many circles. Furthermore, data mining indeed presents difficult challenges, yet these might not be the ones which intuitively come to mind—an insight which calls for further contemplation and analysis.

5.1.1 Data Mining: In Theory and in Practice

5.1.1.1 Data Mining: Definitions, Processes, and General Terms

The term “data mining” has recently been used in several contexts by policy makers and legal scholars. For the discussion here, I revert to a somewhat technical definition of this term of art. Here, data mining is defined as the “nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data.” Even within this definition, there are several intricacies. The term “data mining” refers to both “subject based” and “pattern based” searches (Cate 2008; Slobogin 2008, 323). The former refers to database searches of and for specific individuals, events and predetermined patterns. However, the core of this chapter focuses on the latter forms of analysis (also referred to as “event-based” data mining). These methods provide for a greater level of automation, and the discovery of unintended and previously unknown information. Such methods can potentially generate great utility in the novel scenarios law enforcement and intelligence now face—where a vast amount of data is available, yet there is limited knowledge as to how it could be used and what insights it might provide.

In “pattern based analyses,” the analysts engaging in data mining do not predetermine the specific factors the analytical process will use at the end of the day. They do, however, define the broader datasets which will be part of the analysis. Analysts also define general parameters for the patterns and results which they are seeking and could be accepted—such as their acceptable level of error. Thereafter, the analysts let the software sift through the data and point out trends within the relevant datasets, or ways in which the data could be effectively sorted (Zarsky 2002–2003). The data mining process could achieve both descriptive and predictive tasks. Descriptive data mining provides analysts with a better understanding of the information at their disposal, while uncovering hidden traits and trends within the dataset. When applied by law enforcement to vast databases of personal information, such analyses can uncover disturbing behavior patterns, and assist in ongoing investigation to find criminals and terrorists they are already seeking. While these practices generate concerns, this paper focuses on the use of the data mining of personal information for

---

7 Since the matters addressed here were drawn out elsewhere, the analysis is brief. For a more in-depth discussion, see DeRosa 2004; Zarsky (2002–2003). See also Taipale (2003).

8 For a discussion regarding the distinction among the two—see Cate (2008).

9 For a discussion as to how these data mining techniques are carried out see, Zarsky (2002–2003).
predictive modeling and analysis—an issue which generates far more interest (and subsequent fear).

In a predictive process, the analysts use the data mining application to generate rules based on preexisting data. Thereafter, these rules are applied to newer (while partial) data which is constantly gathered and examined, as the software constantly searches for previously encountered patterns and rules. Based on new information and previously established patterns, the analysis strives to predict outcomes prior to their occurrence (while assuming that the patterns revealed in the past pertain to the current data as well). In the law enforcement and national security context, such insights can prove quite helpful—at times allowing for sufficient reaction time before it is too late.

### 5.1.1.2 Data Mining: Automation and the Human Touch

When considering the detrimental aspects of data mining, the automated nature of the process quickly comes to mind. Therefore, it is important to address the extent of automation and human influence in this process. Counter to what one might initially believe, even with predictive data mining, the role of the human analyst and her discretion is quite extensive. For example, the dataset must be actively constructed, at times by bringing together data from various sources. The analysts also predefine the parameters of the search. These actions directly impact the outcome of the process, and thus policy.

The extent of human discretion involved in this process is not a factor set in stone. Rather, it is a result of various policy decisions. For instance, it is impacted by whether the process is interpretable or non-interpretable. As this term is not commonly visited in the literature, I will devote a few lines to address it. With a non-interpretable process in place, the actions premised upon the predictions the data mining process provides are not necessarily explainable to humans. Namely, the software makes its decisions based upon multiple variables that were learned throughout the data analysis. This process is not easily reduced to comprehensible human language. Therefore, applying non-interpretable schemes affects the role and discretion of the analysts. In non-interpretable processes, human discretion is minimized to setting the parameters for generating predictive algorithms ex ante. The subsequent process of sorting objects, events or people is carried out automatically, with minimal human oversight. Yet perhaps the greatest effect on the role of the human comes after the fact. When a process is non-interpretable, it is very difficult to provide an answer as to why a specific result was reached beyond stating that this is what the algorithm found based on previous similar cases in the past.

---

10 This is done both in advance, and after the fact, by “weeding out” results she might consider as random, wrong or insignificant.

11 I was told by data mining experts that this is usually the case with face and image recognition software.
The flip side of these processes would be a fully interpretable analysis—one that uses a limited number of factors, which in turn could be reduced to a human-language explanation. With interpretable results, an additional stage could be added in which the analyst works through the patterns and criteria set forth by the computer algorithms for the prediction tasks. These could be indications of higher risk associated with individuals of a certain height, age, specific credit or purchasing history—and, of course, the interaction of all these factors. With an interpretation in hand, the analysts can track and set aside factors and patterns which they find offensive, ridiculous and problematic. In addition, the analyst could provide a response to inquiries as to what initiated special treatment of an event or individual. The interpretation process would no doubt prove costly, both in terms of additional expenses for analysts, efficiency and effectiveness lost in the process. However, it provides advantages in terms of accountability and transparency.

Providing for an interpretable process also enables an additional level of human scrutiny in the predictive data mining dynamic. If analysts have a good grasp of the elements used, they can further seek out a theory of causation. Such a theory would go beyond the mere correlation data mining reveals and seek out explanations as to why these are proper indicators beyond the notion that they merely “work.” This step as well can prove helpful in weeding out ridiculous and random findings. It can also block practices which resemble problematic (or even illegal) discrimination.

To summarize, this segment provided a broad overview of the meaning and use of data mining when applied to the analysis of personal information by governments. It also briefly clarifies the extent of human discretion and computer automation. The entire discussion is, however, premised on an underlying assumption that data mining tools are effective in achieving their analytical objectives, while maintaining an acceptably low-level of false positives and negatives. Whether this is indeed true is currently hotly debated (Jonas and Harper 2006; Schneier 2006), and notoriously difficult to measure. The answer to these questions will depend on context, as well as on the costs, consequences and levels of false positives and false negatives. Therefore, prior to engaging in data mining, a relevant authority must conduct an assessment of the effectiveness of the data mining process (TAPAC 2004). If such analysis indicates that data mining schemes are doomed to technical and operational failure, data mining must be abandoned. However, the analysis presented below is premised upon the contrary assumption—that data mining indeed works, and at times even too well.

5.2 The Fears and Challenges of Governmental Data Mining

Data mining presents vast opportunities for bridging the gap between the government’s informational needs and the vast datasets of information at its disposal. With data mining, such data could be transformed into knowledge. However, these practices generate a variety of concerns. These concerns, in turn, are now requiring policy

---

12 However, “building” a theoretical justification to a statistical correlation is usually easy and merely requires some imagination. Thus, one can easily question the extent of protection from arbitrary results a call for “causation” provides.
makers and courts to engage in an extensive discussion and analysis. A discussion of these matters splinters quickly into a multitude of claims and counterclaims. Fully addressing all these issues is beyond the confines of this (or any) article. For that reason, this chapter focuses on a specific methodological point which must be applied in every one of the data mining contexts—addressing alternatives.

Yet, in the interest of providing context, this segment maps out the specific analytical junctures where data mining is challenged. It is at these points where addressing alternatives is crucial. This analytic mapping relies upon scholarship and policy reports addressing such matters in the last few years. For the sake of clarity, I distinguish among the different steps of personal information flow such as the collection and analysis stage and the usage of personal data.13

The following description is mostly theoretical and normative, with only limited attention provided to positive law. I chose this analytical path for several reasons: First, temporarily setting aside the positive analysis allows for quickly working through the relevant issues, and leaving room for an in-depth discussion of the alternatives below. As the law greatly differs among jurisdictions, a full-blown analysis of positive law would be lengthy and complex. Second, to a great extent, the legal and policy standing on these issues is still up for grabs. In the United States, most of these issues have not been decided upon in the courts and are waiting for regulation and legislation. They probably do not amount to breaches of constitutional rights—or as Daniel Solove succinctly summarized—“...data mining often falls between the crevices of constitutional doctrine” (Solove 2008, 355). They are also probably permitted according to current privacy laws in view of various exceptions and loopholes. Yet public opinion and various policy groups do not approve these practices (Slobogin 2007, 194)14—and thus some changes in the law are inevitable. In Europe, the entire legal structure governing privacy and data protection within government is being revamped as part of the Lisbon Treaty’s aftermath. Yet new policy will surely follow as both privacy and data protection are recognized as basic human rights. Therefore, a discussion at a high level of abstraction is still fitting.

Collection and Analysis A data mining process inherently calls for automatically reviewing and analyzing profiles filled with personal information regarding many different individuals. This process will be carried out without their consent to such analyses. The data used was previously collected by either government or commercial entities. It is hard to imagine that individuals’ conceded to the data mining process here described at the time of collection, or at a later stage. If the information was collected by government, citizen might not have conceded to data collection at all. Rather, they were forced to provide their data and settle for a basic and vague notice of the collection and future uses provided by the government.15

---

13 Transparency is an additional category which requires scrutiny and discussion, yet it calls for a very different form of analysis. For more on this issue, see Zarsky (2012).

14 For an empirical study pointing in this direction, see Christopher Slobogin (2007).

15 In the United States, such rights are governed by the Privacy Act, which call for the publication of SORNs to notify the public of such uses. For more on this, see the Privacy Act Overview of 2010, accessed July 12, 2011, http://www.justice.gov/opcl/1974indrigacc.htm.
Engaging in personal data analysis without the direct consent of relevant data subjects runs counter to several legal concepts in the context of privacy and data protection. First, such actions might constitute searches (Blitz 2011; Slobogin 2010). If so, data mining will be considered an illegal search when carried out without sufficient judicial approval—approval which is not currently sought. According to other privacy theories, which are more central in European thought, data mining without prior consent constitutes a violation of the realm of control individuals have over their personal information (Solove and Schwartz 2006; Westin 1967). The information is also analyzed and used outside the original context in which it was collected, thus violating the principles of “Contextual Integrity” set forth by Nissenbaum to describe proper information uses and flows (Nissenbaum 2009). Currently, under US law at least, such practices are permitted if the data were collected legally and a very general and vague notice is provided (TAPAC 2004).

On a more pragmatic level, these vast analyses projects might generate a “chilling effect” with regard to many important human activities and behaviors; if citizens fear that specific actions will generate additional governmental scrutiny, they will refrain from these actions—such as travel, communications or consumption—even when they are legal and at times socially beneficial (Cate 2008; Solove 2001; Strandburg 2008). From a somewhat different perspective, knowledge of such actions impedes upon the citizens’ autonomy; it does not allow them to develop their “self” to the greatest extent possible.

Finally, even if these practices are justifiable in one context, such as that of homeland security, there is the fear that government and its agents will not stop there. Equipped with these powerful tools and immense datasets, they will use them for other, more mundane, objectives. While data mining could be justified to protect citizens from upcoming risks which might lead to devastating outcomes, it probably cannot be justified as a tool for locating deadbeat dads. This is the “Project/Function Creep” concern, which has many commentators and policy makers worrying. This concern might lead to recommendations that data mining projects should be stricken down in their entirety (Slobogin 2008, 326).

---

16 This is not the classic understanding of a “search,” which does not pertain to searches of data which were already collected. However, newer theories reexamining the “search” terminology question such wisdom. Slobogin, for instance, believes the term should be used in the same way the public understands it. According to his empirical studies, that includes data mining. Mark Blitz is also examining whether searches within data or other sources the government obtained lawfully could be considered a “search,” nonetheless, while focusing on DNA samples.

17 The notion of “privacy as control” was set forth by Alan Westin and implemented in various elements of both the OECD Principles and the EU Data Protection Directives. See generally Westin (1967); on the EU Data Protection Directives in general, see Solove and Schwartz (2006).

18 For a discussion of this argument in the Data Mining context, see Cate (2008) who notes it as perhaps the most powerful one in this context. Strandburg makes a similar argument, while pointing out that in some contexts data mining might impede on US Constitutional First Amendment Rights, such as freedom of speech and association. For a general discussion of privacy and autonomy, see Solove (2001).
Usage Using the knowledge derived from the data mining process for various governmental objectives generates an additional set of problems. A basic concern is that the outcomes will be used to unfairly discriminate among citizens. Discrimination could prove unfair for a variety of reasons: it could be premised (at times, tacitly) upon unacceptable social factors, such as race and nationality. It could also be premised upon partial information, or immutable factors, over which individuals have no control. In addition, some might object to distinguishing among individuals based on mere correlations with others (who might have committed wrongdoings), as opposed to the specific thoughts and actions of the relevant individual. This is the generalized/individualized suspicion distinction some scholars have already considered (Slobogin 2007, 40).\(^1\) I am currently unaware of specific laws addressing discrimination by governmental (Harcourt 2007; Schauer 2006)\(^2\) data mining in the United States (beyond the protection provided through the Equal Protection Clause to all). In the EU, specific rules governing automated searches might apply, and indeed provide individuals with additional rights to learn the internal process used (Korff 2011).\(^3\)

An additional concern often mentioned when addressing the data mining process, is that it is ridden with errors. These errors can be of different forms and come at various stages of the process: they can result from errors in the initial data, in the aggregation process,\(^4\) as part of the statistical modeling and computer programming, in the implementation of the system or in the ability to correctly define the risks and match them to the strategies on the ground. The errors can have devastating outcomes. First, they can render the entire process ineffective and inefficient—unable to identify real risks while leading law enforcement to follow bogus leads. Yet even when setting these concerns aside (and assuming they can be tested), errors can have detrimental effects on specific individuals; these might be subjected to discomfort, additional scrutiny and even castigation and suspicion by others for no real reason.

It should be noted that data mining tools maintain the ability to self-correct errors in the analysis process. As the process rolls on, information regarding success rates, false positives and false negatives becomes available and is “fed” into the process. Analysts can use such data to fine-tune the algorithms they later apply. In addition, data mining techniques could be used to study the datasets and seek out information which does not fit other data patterns. Analysts could then examine whether anomalies in the data result from errors and correct the database accordingly.

Finally, lack of knowledge and understanding of the data mining internal processes might also raise fears related to “due process” (Steinbock 2005)—or lack thereof. Individuals might fear that adverse action was or will be taken against them without

\(^{1}\) For a discussion and critique of this distinction, see Slobogin (2007).

\(^{2}\) I intentionally emphasize the lack of laws in the governmental realm. In the commercial realm there is some reference to this issue in the Fair Credit Reporting Act. For a critique of this situation and a call for a change, see Harcourt (2007). For a very different perspective, see Schauer (2006).

\(^{3}\) For a full discussion of this issue in EU law (as well as the law in the various states) see an excellent discussion in Korff (2011)

\(^{4}\) For a discussion of errors in general and of this context in particular, see Ramasastry (2004).
their ability to examine the reasons or challenge the allegations. The data mining process might be inherently opaque and its inner working hidden from the public for various reasons. Lacking a better understanding of the internal process encumbers the individual’s autonomy and compromises the interests “due process” rules are set out to protect.23

5.3 Alternatives to Data Mining

Indeed, it has been said that democracy is the worst form of government except all those other forms that have been tried from time to time

Winston Churchill

5.3.1 Mapping out Alternatives

As the previous segment shows, a policy analysis of the data mining of personal information is an extremely complex matter. A comprehensive analysis calls for addressing all these elements, and more. In addition, however, a policy study of data mining must consider the alternatives to applying data mining analyses. These are the policy strategies of choice, to be set in place if society refrains from applying data mining. As the quote above demonstrates, examining an issue without considering its alternatives is a futile exercise. In this section, I will briefly present the following five alternatives: (1) altogether refraining from the analysis of personal information to identify individuals and events of higher risk and therefore treating all individuals and events equally; (2) differentiating among events and individuals randomly; (3) doing so while relying on the human discretion of field officers, who examine personal information pertaining to the specific individual; (4) relying upon profiles and patterns constructed by experts and (5) applying data mining only to anonymous or anonymized data.

These alternatives are not without overlaps. Solutions might include elements from some or all of these options. Rather than alternatives, these are trajectories for various policy strategies which could be implemented—with every “alternative” pushing a different form of compromise. An understanding of the solutions’ pros and cons along these lines, prior to selecting one of them for further implementation, is imperative. The analysis presented here assists in carrying out such balancing.

(1) The first and most obvious alternative to government data mining initiatives is altogether refraining from the analysis of personal information to identify individuals and events of higher risk, and setting them aside for specific treatment. Generally, this is the alternative to data mining usually envisioned. Yet as I will explain here, it is probably the most unlikely strategy to follow.

23 US “due process” doctrine does not apply for various reasons. In some contexts, EU law provides for a right to understand the processes’ internal workings. For a discussion of this issue, see Steinbock (2005).
Setting aside technologies and policies that enable selection will lead to treating all individuals (or events) as potentially risky and subjecting everyone to higher scrutiny. When this happens, however, the potential risk transforms into inefficiencies and discomfort, as well as excessive governmental costs. These costs will no doubt come out of resources that could have been used to have a better society (or left in the pockets of the taxpayers). This strategy might also lead to difficult legal questions regarding the authority to subject all individuals to additional burdens when no evidence indicating elevated suspicion against them exists. Finally, such course of action could lead to substantial breaches in security and system failures. The fatigue resulting from applying higher security standards to individuals and events that are clearly of low risk will adversely impact the alertness of the relevant officials. These officials, at the end of the day, might miss or react poorly to an actual threat when it finally comes their way.

Deciding whether to opt for this option, as opposed to using data mining, calls for a difficult balance of interests. It also requires tough decisions as to whether society should adopt an initiative which will risk the inconvenience, harm and even liberty of specific individuals at several junctures. It must note that this alternative leads society in its entirety to be taxed, either financially, in terms of attention, or even raising risks of security. Clearly, liberal and democratic societies should be willing to refrain from any data analysis if balancing indicates this is necessary. Furthermore, society is mandated to do so (Schauer 2006) when important interests of the specific harmed group are at stake. This is the case when governmental practices intentionally discriminate on the basis of race or nationality. Yet in other instances which do not involve the risk of reinforcing very problematic stereotypes, balancing becomes far more difficult and the results far less clear. In many instances, governments will decide that applying some form of selection and focused attention is prudent.

Yet beyond the normative balancing, this first alternative is politically unsustainable. As risk manifests and law enforcement resources are stretched, politicians and policy makers will face great pressures to “do something” with the vast datasets of personal data at their disposal. Thus, they will be pressurized to move away from this alternative. Given the high risks and limited enforcement resources, a form of selection must transpire. The question is, of course, how the selection will take place. This is where data mining and the other options come into play.

(2) Refraining altogether from selective practices in the context of security or law enforcement is unreasonable and unfeasible; the costs might be too high (costs that might lead to compromising basic rights of many citizens) (Slobogin 2007, 2006).

24 It would mean that all individuals, for instance, would be required to arrive 30 minutes earlier at the airport to go through heightened security checks.
25 For instance, discrimination on the basis of “sensitive information” such as race is illegal, even when such discrimination is statistically justified. For a partial critique of this outcome, see Schauer (2006).
and the fatigue to the system too great. This leads to considering alternatives which enable the selective allocation of resources. This second alternative applies randomness to meet the security risks at hand (Harcourt 2007). Searches, stops and other steps of enforcement would be applied to random individuals by the relevant field officer.

Scholarship points to this option as either a strategy that must complement data mining profiling or replace it entirely (Harcourt 2007). Random allocation and testing is an important measure to be applied in conjunction with data mining analyses (or any other strategy). It is crucial for statistically monitoring the effectiveness of data mining initiatives and examining whether they are justifying the compromises they entail. Here, however, I am referring to a much broader implementation of random allocation and a much narrower role for data mining.

While broadly applying a random scheme when specific personal information is available for analysis might seem as a strange (to be polite) option, in some contexts it certainly might suffice. When carried out in public, random checks might achieve sufficient deterrence of criminals and others fearing to be singled out. It will also allow government to show it is doing something—or in other words create a “security theater” (Schwartz 2008). By doing so, governments will sidestep many of the problems data mining present, while also averting the problems of fatigue and overstretching of resources.

With randomness, as with almost any strategy, there are several crucial details which must be attended to. First, there is the actual chance of being randomly selected. A very low chance due to limited law enforcement resources will probably fail to achieve deterrence. A very high chance will begin generating the problems of alternative (1). Another issue is how “randomness” would be achieved. While this might sound trivial, in fact, it is quite difficult for individuals in the field to engage people randomly. They are quite often affected by internal biases and external factors (notions to be explored in depth below) when striving to make a random selection. This, of course, leads to unfair outcomes on the one hand and the fear of gaming and ineffectiveness on the other hand. For a random search to be truly random, a randomizing tool must be applied—a computerized gadget that will indicate when someone would be selected, stopped or questioned. Training field agents to ignore their judgment and succumb to a random number generator will not be simple. For all these reasons, administrating randomness might not be as easy as one might think.

26 For instance, one might argue that encumbering the ability of all individuals to travel when striving to provide for security might limit their freedom of movement. I will refrain from developing this notion. For more on this point, see Slobogin (2007, 102).

27 An option promoted by Harcourt (2007).

28 When the chance for selection is very low, such enforcement loses its teeth, as the penalties inflicted cannot be disproportionate to the specific transgression. See similar dynamics occurring in the music and film industry when striving to enforce their rights online.

29 Clearly, just selecting every tenth person or a similar strategy will allow easy gaming of the system by interested parties (all they have to do is travel in pairs and one of them will surely be beyond suspicion!).

30 I thank Kathy Strandburg for making this point.
Yet even if these problems could be resolved, I believe the “random” alternative is unfeasible. Engaging in mere random selection, when a great deal of information which could be of relevance is available, might be hard for the public to swallow. The notion of ignoring information on the one hand, and subjecting individuals who are clearly of a very low risk to a higher level of scrutiny on the other, would be difficult to accept politically and might even make a mockery of the entire process. At times, the public must overcome its aversion of solutions which generate such “intentional blindness” for reasons detailed above (such as avoiding racial discrimination). Yet there is a paucity of strong justifications for applying randomizations broadly.

(3) The third alternative concedes to both the need for specific treatment of individuals and the use of personal information in this process. With this alternative, a decision maker examines specific personal information about an individual and makes an informed, ad hoc, decision. The decision maker might rely on the information she directly collects at the time of a personal encounter (what the individual is carrying, doing, saying). Yet she might also rely upon information in the individual’s governmental profile when making this decision (What has he done? Where has she been?). In most cases, the decisions made in this scheme involve a field officer or a lower-level bureaucrat exercising their discretion. Possible examples are tax officers selecting a return for audit, security officers deciding which individuals to subject to additional questioning, or police officers deciding what street to walk or drive by (Slobogin 2007, 23).

To further explain the nature of this alternative, it is important to note what decision makers are not doing. First, they are not running analyses which involve the datasets of the entire public (and thus individuals entirely removed from the relevant context). Second, the process is not automated (in the computerized sense), although the decision maker might use a computer to view personal information about the subject in real time. Third, it does not involve the formulation of factors, representing statistical groupings which indicate a higher or lower level of risk (at least not intentionally or explicitly). In addition, this alternative might have operational advantages. It requires officials to think on their feet, as opposed to some data mining schemes which require individuals to merely apply an algorithm. This latter role might adversely impact official’s motivation and performance (although the motivational problem could probably be resolved with alternative measures).

In its most basic form, this alternative is merely hypothetical. Governments no longer operate in this way. Field officers never have full discretion, but are subject to protocols, which are a result of central planning. Allowing full discretion and lack of any protocol is simply unthinkable given the inability to control and regulate the actions of these officers, which might open the door to massive abuses (Slobogin 2007, 123). In addition, opting for this alternative will call for ignoring a great deal

---

31 The discussion is intentionally avoiding instances in which the actions resulting from the higher level of scrutiny constitute searches, or other actions which directly impede upon the liberty of the subjects. I am doing so to sidestep the broader discussion about Terry stops and other such actions, where “reasonable cause” or other levels of scrutiny are mandated. For a mapping of these contexts, see Slobogin (2007, 23).
of knowledge within the system—knowledge which one field officer cannot integrate effectively. When neglecting to make use of such additional information, existing threats will not be sufficiently met, and potential evil doers will easily circumvent security measures by hiding their intentions.

For these and other reasons, addressing and critiquing this option might resemble attacking a straw man. However, there is still merit in examining this practice, even in its purest form. While this alternative is probably rarely exercised or even advocated, policy choices will no doubt reflect some variation of it. The options which are finally selected will be somewhere along the continuum between this alternative and the next one to be discussed (“4”). In other cases, some balance between this option and a data mining-based system which provides officers with recommendations, will be applied. Therefore, this alternative’s pros and cons must be accounted for.

It is also important to point out that these practices are not as distinctively different from the use of profiles (to be addressed below) or even data mining, as they purport to be. The difference between them is one of degree, as in this model greater importance is vested with individual discretion. On its face, this alternative seems to be distinctively different, while treating every individual separately, and reaching conclusions while relying on data pertaining to the relevant subject. It is perhaps the most salient example of “individualized suspicion” (as opposed to generalized one). However, every future-looking statement pertaining to one individual’s risk and prospects is actually premised upon a statistical analysis (even if it is an unconscious one) of the behaviors of others (Schauer 2006). The prediction is carried out within the minds of the field officers, who generate it on the basis of behavioral patterns they witnessed or learned of in the past.

In addition, the policy structuring the law enforcement framework which leads to the field officer’s discretion is based (at times, quite subtly) upon predictions. These predictions, in turn, were premised on some form of statistical analysis. In some cases, field officers are instructed that relatively minor crimes or actions (such as carrying box cutters) are indicative of other, more serious crimes (such as commandeering aircrafts). This rule is in fact a prediction premised on previous findings and behaviors. In other instances, field officers are required to present specific tests or questions and study the results they receive. Again, these questions and tests were structured with previous encounters in mind and an assumption that similar behavior patterns will reoccur.

To sum up our introduction to this alternative, let us examine two important parameters which were previously introduced: interpretability and correlation/causation. On its face, the process involving this alternative is interpretable. It is possible to learn the reason for any specific decision simply by asking the decision maker (and steps could be taken to assure that decisions would be logged to assure effective retrieval). Thus, this aspect provides an important advantage over the data mining practices which might lack interpretability. Yet the interpretability of this alternative could be called into question; the reasons the officials or field officers report might

---

32 For instance, if the officer focuses on someone with a gun, it is because he created a mental profile with the category “people with guns,” and is focusing his attention on those within that category.
not be the true ones (and there is almost no way to verify them). In addition, if the officer states that he relied on a basic intuition or hunch (which might be the case in many instances), the decision is virtually uninterruptible.

A similar observation could be made regarding the correlation/causation divide mentioned above. On its face, the field officers will refer to theories of causation when applying various decisions and measures. This will provide a safeguard against unfair or erroneous policies. However, when law enforcement decisions are opaque and rely upon intuition, they might be merely premised on assumed correlations the relevant official noted in the past, which have yet to be backed by a relevant theory (or even authenticated empirically). Thus, a closer look at this alternative shows that it is not as promising as we might have originally thought.

(4) The fourth alternative to data mining requires law enforcement to rely upon predetermined profiles for the allocation of resources and risks among individuals and groups (Schauer 2006, 166). This profile is constructed by experts, who apply their common sense, expertise and experience to the task, in a top-down process. Experts will set up parameters for selecting tax returns, individuals at borders or the location of police cars. They will do so while working through datasets of previous actions and perhaps other forms of knowledge sets from the social sciences.

The differences between this alternative and data mining (as well as the former) could be set along three themes. First, the process does not call for “combing” through the entire dataset of personal information available to the government in the same way data mining applications operate (yet surely to a greater extent than the previous alternative). Note, however, that the profiling stage calls for some examining of datasets pertaining to previous problematic acts. In addition, the general parameters of personal datasets will be reviewed, to get a sense of the “normal” levels of the parameters used, so that a profile of deviations from the norm could be constructed.

Second, the process will not be automated but generated by human discretion. As opposed to the previous alternative, this process is triggered by the discretion of experts. Obviously, this option calls for some use of technology—a system will provide the decision maker with relevant facts, perhaps even with recommendations. Yet the final decision would be of the experts. In addition, the focus of discretion in this context is quite different than the one explored in the previous example; discretion is centralized, as opposed to being dispersed on the periphery of the bureaucratic infrastructure which is what the previous alternative called for.

The third difference between this alternative and the previous one (and a theme it shares with data mining) pertains to the notion of relying on statistics and an “actuary model.” This model uses “generalizations” while making decisions regarding specific individuals. Here, analysts create groups and subgroups of individuals based on set parameters. These groupings instruct law enforcement to treat those within it differently. Such modeling relies on specific assumption regarding the ability to predict the future behavior of individuals, as well as deduce it from the actions of

33 As Schauer explains, such practices are wide spread, and applied by customs, as well as by the IRS; see Schauer (2006).
others. It also accepts the risk of wrongfully treating an innocent individual who happens to fit within a problematic group or profile.

I again conclude this segment by returning to the elements of interpretability and causation. As opposed to the options explored thus far, with this alternative, the process will not only be inherently interpretable but will usually rely on various theories of causation for explaining the elements it includes. This will arguably enhance the autonomy of those subject to the analysis; there will always be an understandable answer to explain the singling out of a specific individual. It will also promote transparency in the procedure, which could be easily explained as a logical thought process. Finally, relying on causation will, as explained above, provide a check against problematic forms of discrimination and errors. This is an important benefit of this alternative, although interpretability and causation could be designed into data mining tasks, if deemed important.

(5) The fifth and last alternative already accepts the ability of data mining to achieve the objectives at hand. However, it requires that the analysis is conducted using anonymous (or anonymized) datasets. This recommendation, set forth by several recent policy reports (TAPAC 2004; Markle Foundation 2003), calls upon the government to engage in the analysis through the usage of several cryptographic tools. These tools allow for data matching, warehousing, and even mining, without providing the analyst with actual access to the personal information being mined. Access to personal data could be provided at a later time if suspicion arises, yet safeguards could be set in place to block unrestricted data sharing.

This alternative calls for a different form of balancing. It mitigates only some of the problems of data mining, while leaving others unaffected or even exacerbated. This strategy might reduce some forms of privacy and autonomy-related fears, as the public’s concerns of being searched and tracked will be eased by knowing the government cannot connect their personal data to their real identity (Slobogin 2007, 195). However, this alternative increases the chances of errors within the process and the lack of transparency. In addition, concerns regarding the practices which follow from data mining—the generation of patterns which would later be used to unfairly distinguish among individuals and events as parts of groups—will still persist! Finally, applying this alternative comes with non-trivial costs (in terms of both real out-of-pocket costs as well as costs of errors and engaging the system with additional process).

Considering this alternative also requires some rethinking as to the actual protection anonymity provides. Recent studies have indicated (Ohm 2010) that a massive anonymous database of personal information, which includes a multitude of factors about every individual, can be re-identified by sophisticated users if another database of identifiable personal information is at their disposal (Ohm 2010, 1746–48). Thus, the government would probably be able to circumvent the protection measures mentioned here, should it choose to do so. These new findings weaken the attractiveness

---

34 For empirical findings showing this point, see Slobogin (2007, 195).
35 This was the case in the Netflix/Imdb fiasco. Such multi-factored datasets are now at the disposal of many public and private entities.
of this alternative. However, in the governmental context at least, these concerns of hacking and circumvention are probably manageable though various technological tools and disciplinary measures which will limit access and control the data.\textsuperscript{36} All in all, however, this fifth alternative still requires a great deal of additional consideration.

5.3.2 Distinguishing between the Field Officer, Profiler and Data Miner

Three key alternatives enable government to engage in selective enforcement and scrutiny: data mining and alternatives (3) and (4) above. There are key differences between these options—differences which have crucial policy implications. In this segment, I will examine with greater depth the differences among them. The points made here can be used in future analyses of data mining and its alternatives, which must account for these elements and the differences they generate. Of course, in varied contexts, these differences will have different implications—yet a basic understanding of this framework is imperative. I also point out which differences are not crucial to the discussion, but can prove to be a distraction from addressing other important elements.

First, let us take a look at the notion of human discretion and the different methods of decision making the models employ. More specifically, the alternatives lead to a choice between various forms of human discretion, as well as a balance between human and automated discretion. Selecting between methods of discretion has several implications. The most central one is the forms of errors it generates.\textsuperscript{37} If one form of discretion generates predictable errors (even if those are not substantial) the system would be easily gamed and manipulated. If the errors are systematic, a specific set of the population would be harmed, leading to distributive and other harms (again, even if overall efficiency is maintained). If the errors are both systematic and detrimental towards specific segments of the population, which are either weak or were singled out in the past, this leads to an additional set of problems. When balancing alternatives against each other, the errors resulting from the different forms of discretion must be accounted for. The next few paragraphs briefly map out how that could be done.

Preferring human discretion, as opposed to deferring to the output of a data mining-powered application, leads to at least two shortcomings (which pertain to

\textsuperscript{36} This option still holds substantial benefits, as it minimizes the risk of illegal abuse of the information by a government executives (such as the many stories occurring every year of tax officials sharing or selling personal information about citizens). Note, however, that this problem could also be mitigated through disciplinary actions.

\textsuperscript{37} If one form of discretion generates errors which are frequent, the entire process is compromised. However, let us assume that the threshold of a reasonable level of errors would be attended to as a preliminary matter—and if the level of errors will be unacceptably high, the project would be set aside. Yet as I demonstrated in the text, even with an overall acceptable level of errors, problems can still prevail.
almost all decisions premised on human cognition) that quickly transform to errors in the final outcome: Human decisions: (a) tend to rely upon heuristics and (b) at times employ hidden biases. Both dynamics are systematic and predictable. The latter also generate errors detrimental to specific weaker and vulnerable segments. I now turn to take a closer look at both elements, explain how they generate differences between the models and briefly note the implications of these differences.

A vast psychological literature regarding heuristics clearly indicates that when dealing with complex tasks, the human brain applies various shortcuts which allow it to overcome information overload (Korobkin 2003; Tor 2008). These rules of thumb often lead to correct decisions. However, at times, heuristics lead to predictable errors. This occurs when individuals face the need for quick decisions, with limited attention and vast information to consider. While some errors could be corrected through training and experience, many others cannot.

Considering the alternatives pointed out above quickly leads to recognizing flaws in the third alternative, which relies heavily on the individual discretion of field officials. This alternative will lead to predictable cognitive traps where heuristics will be applied but lead to a wrong result, which adversaries might abuse. Thus, for this reason alone, opting for this (third) alternative will come at a high price in terms of efficiency and fairness. When opting for the forth alternative (expert-driven profiles), this concern is somewhat mitigated. Experts might have greater awareness to these tendencies to err, and focus on empirical findings, rather than mere intuitions. They also need not make quick decisions under pressure. However, this process could be inflicted with heuristic-related errors as well, given the reliance on human-based discretion.

On the other hand, data mining faces the least of these troubles. Computers have no need for shortcuts and heuristics when they have the capacity to address all data. When indeed, for efficiency purposes, only segments of the data are addressed or another analytic shortcut is used, it is a shortcut the operators are well aware of and can take into consideration.

Relying upon discretion also allows for the internal biases of the individual decision makers to impact their actions and decisions, even inadvertently. At times, the discrete decision of the experienced decision maker is a discriminatory one. Such discrimination is premised upon (at times, subconscious) animosity towards specific segments of the population, or other forms of prejudice. This might result in an inefficient outcome (Schauer 2006, 179). Far worse, however, this might lead to unfairness towards the weaker segments of society, or against groups society designated as protected.

Biases can transpire within the frameworks of both the third and forth alternatives. Field officers are most susceptible to generate these distortions. Indeed, a recent review of studies addressing law enforcement field decisions with regard to race

---

38 This was exactly, according to Schauer, the case in O’Hara airport, where it was revealed that the percentage of minorities made subject to intrusive cavity searches was very high. When such practices, which were no doubt motivated by racial animosity, were stopped, the success of such searches increased. See Schauer (2006).
shows an alarming and distorted picture (Harcourt and Meares 2010). For this reason, providing full discretion to field officers is unthinkable (Harcourt and Meares 2010). Yet even relying on expert decisions (as in alternative #4) might not resolve many of these concerns. Experts might be plagued with internal biases and generate policies which are unfair to weaker and protected groups. Rather than relying upon strong data findings and expertise, they might be motivated by beliefs and prejudice. Note, however, that the fourth alternative has the advantage of a central process. As opposed to a system where decisions are made at the periphery, the expert profiles could be closely audited and studied in an attempt to identify arbitrary conduct that might lead to unfair discrimination. This, of course, is easier said than done.

With data mining, applying an automated process allows the central planner to retain better control over the actions in the periphery as well. Yet data mining provides an additional benefit; computer modeling is not driven by human assumptions (which might be both hidden and biased) but by the data itself. Therefore, concerns regarding hidden biases premised on prejudice might be sidestepped by applying data mining.

Many will disagree with this last statement. Beyond the fact that data mining has systematic flaws, hidden biases might be a feature of data mining, and lead to even graver concerns. These biases might be put in place at the points of human interaction listed above, which in many cases are hidden from public scrutiny. Thus, data mining allows for the embedding of values as well. The difference between the options here discussed amounts to the ease of embedding values ex ante and the ability to identify these instances ex post. Those arguing against data mining will state that biases can be built into decision-making processes quite easily ex ante, and are difficult to identify, if hidden well, after the fact. For that reason, data mining runs high risks of generating biased conduct.

I believe, however, that the problems mentioned are not inherent features of data mining, and certainly are not beyond repair. If the data mining process is sufficiently transparent, it can effectively overcome these challenges. Adding interpretability and even causation to the data mining process could allow policy makers to assure that biases are averted. In addition, analysts could keep a close eye on the forms of software used, and the protocols applied when using it. Biases in a central computer code, once acknowledged, could be tackled with ease and identified effectively by external review. This task is certainly easier to tackle than achieving this objective with the other alternatives mentioned. Managing and mitigating hidden biases in the actions of numerous field officers vested with a great deal of discretion is a much harder task. This would call for tracking, evaluating and disciplining all actions carried out in the periphery. Even doing so with a group of central experts seems daunting, and will generate numerous painful confrontations. For these reasons, I

---

39 The authors explain that part of the role of the 4th Amendment is to limit the discretion of law enforcement. Harcourt and Meares (2010).

40 I acknowledge that even when using a central system, some level of examining of the actions of the periphery operation is needed as well. Yet this would be substantially less than the level required in the third alternative model.
believe this segment of the analysis clearly points to the superiority of data mining initiatives.

A second difference between these central alternatives pertains to the use of decisions premised on statistical groupings, as opposed to individualized suspicion. Deciding on the basis of a group’s statistical analysis leads to a much broader debate, in which some scholars show great resentment to the “actuary method” (Harcourt 2007). This is the notion that individuals are treated as parts of groups, which have specific predefined traits and parameters, as opposed to actual clinical work to examine the relevant situation. Similar methods are broadly adopted in many stages of modern life (especially in insurance), and generate aversion there as well. Unlike the previous issue, this one should not weigh heavily when balancing alternatives.

While using this form of statistical analysis in data mining might generate negative sentiment, I believe categorically rejecting the “actuary method” is unwise. Merely relying on an individual’s record, not only is inefficient, but includes implicit reliance on groupings as well. In addition, the individualized process generates several crucial detriments, especially the lack of interpretability and transparency. Therefore, when opting for “individualized” treatment, the public does not always understand the process’s underlying assumptions and inner workings. Options which use statistical analysis (such as alternative (d), or data mining), might indeed be rejected, but it should be for other, more specific, reasons.

The third issue is that of automation. Deciding between the alternatives mapped out above is again merely a subset of a broader discussion concerning the role of computer-generated decision making in a technological society (Bamberger 2010). Data mining calls for a great deal of automated decision making, while the other options do not. Philosophically, those fearing automated decision making show disdain for the tyranny of computers, which might make systematic errors and are unable to take into account the delicacy of the human condition. They also fear that society does not easily accept errors made by computers, as opposed to easily accepting that “to err is human.” Finally, they might consider the notion of individuals treated by computers (as opposed to fellow humans) as undignified (Korff 2011). These are all powerful arguments against the spreading use of data mining. Yet again I do not believe these distinctions, on their own, should receive a great deal of attention when comparing alternatives.

When addressing this issue, we must always worry that behind many of the arguments stated in the previous paragraph, stands a fear of technology with a neo-Luddite flavor. In other cases, these arguments might result from a tendency to underestimate technology and its ability to match human achievements. However, the analysis of alternatives presented here shows that non-automated decision making features substantial problems as well. Yet it would be wrong to reject the notion of unease with computerized decision making in its entirety. The public’s resentment towards data mining could be a result of an irrational fear of automation. Yet, this sentiment might be derived from other strong and meaningful sources which we must diligently seek out and explain—among others the fear of errors, loss of autonomy and the lack of

---

41 For a discussion of this matter in the Corporate Risk Management setting.
transparency. After uncovering these concerns, they must be tackled directly. The broader, somewhat vague, notion of automation must be set aside, especially when accounting for the balances alternatives entail.

5.4 Conclusion: Alternatives as Building Blocks for Future Analyses

This chapter strived to illuminate a crucial methodological step which can assist policy makers seeking balances in today’s world of global insecurity. Such policy makers are now charged with structuring schemes for using databases of personal information to promote law enforcement and stability. In doing so, policy makers will be called upon to assess the option of data mining. The first step of this process calls for understanding the technology at hand. The second step the analysts face is identifying the variety of problems and questions these methods generate. The third step is introducing alternatives and illuminating the differences between them. These steps formulate a novel methodology for examining data mining practices. Comparing among alternatives will provide for a better sense of the balances and realistic compromises required at every juncture. The comparison must account for all the elements of the discussion. It should account for legal analyses, economic costs, technological abilities, and psychological limitations.

Existing risks call for the use of personal information in an effort to preempt possible harms and attacks. Society will be forced to decide among several non-ideal options. At the end of the day, the solution finally chosen would no doubt be a compromise. The methodological steps presented in this chapter strive to assist in these balancing efforts, while acknowledging that there is still a great deal of work to be done. I hope this small contribution promotes this broader objective.

Acknowledgments This chapter is part of an NWO-funded research project “Data Mining without Discrimination.” I thank Kathy Strandburg, Richard Stewart, the participants of the NYU Law School Hauser Research Forum, the NYU Privacy Reading Group and the DePaul Law School CIPLIT presentation for their comments. I also thank Talya Ponchek for her comments and research assistance. For an extended version of the ideas presented here, see: Zarsky, Tal Z. 2012. Data Mining and its Alternatives Penn State Law Review 116(2):101.

References

Blitz, Mark. 2011. Warranting a closer look when should the government need probable cause to analyze information it has already acquired? PLSC 2011 Workshop. Draft, on file with author.


