The Invisible Worm and the Presumption of Guilt

Robert Sykora

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation
THE INVISIBLE WORM AND THE PRESUMPTION OF GUILT

Robert Sykora†

I. INTRODUCTION ........................................................................................................ 723
II. IMPERFECT DATA IN, IMPERFECT DATA OUT ............................................ 728
   A. Government Technology is Infallible, Right?............................................. 728
   B. Our Courts’ Reliance on Names and Dates of Birth to Identify Defendants: An Inexact Science ................................................................. 729
      1. Birth Date Inaccuracy ........................................................................... 729
      2. Name Inaccuracy .................................................................................... 730
   C. Our Ability to Move Data Rapidly Has Outpaced Our Ability to Understand It ........................................................................................................... 734
   D. Where There’s Smoke, There’s Guilt ......................................................... 735
   E. Openness in Government Meets the Internet ............................................. 736
III. THE NEED FOR A SOLID SET OF STANDARDS TO GUIDE USE OF CRIMINAL JUSTICE SYSTEM DATA ..................................... 737

1. An esteemed colleague (who is an English major to the marrow of his bones) contemplates the creeping, insidious effect of unregulated data mining and is reminded of the invisible worm in this poem by William Blake:

   The Sick Rose
   O Rose thou art sick.
   The invisible worm,
   That flies in the night
   In the howling storm:
   Has found out thy bed
   Of crimson joy:
   And his dark secret love
   Does thy life destroy.

† Robert Sykora is a Minnesota attorney who has worked in the county and state public defense systems since 1983, currently serving as Chief Information Officer for the Minnesota Board of Public Defense. Sykora worked “on loan” at the Bureau of Criminal Apprehension during 2008 as an information policy and technology consultant. He earned his J.D. at William Mitchell College of Law in 1986 and a Master in Public Administration degree at Harvard’s Kennedy School of Government in 2005. The author is grateful for the expertise of Sarah Kurachek, whose meticulous research made this article possible.
IV. STATE LEGISLATURES’ ATTEMPTS TO APPLY FAIR INFORMATION PRINCIPLES ..................................................... 739
A. The Transparency Principle in State and Local Regulation. 739
B. The Opportunity-to-Correct Principle in State Regulation..... 743
C. The Reliability Principle in State Regulation ....................... 745
D. Control-of-Use Principle in State Regulation ....................... 752
   1. Prohibiting Use of Non-Conviction Arrest Records for Other Purposes ............................................................ 752
   2. Controlling Downstream Use by Mandating “Data Babysitting”................................................................ 759
   3. Discourage Use for Casual or Frivolous Purposes........... 764

V. MINNESOTA’S PROGRESS TOWARD APPLYING FAIR INFORMATION PRINCIPLES TO COMMERCIAL DATA MINING OF CRIMINAL JUSTICE SYSTEM RECORDS ............................... 766

VI. CONCLUSION ......................................................................... 768

I. INTRODUCTION

A mother jumped when she saw the sheriff’s deputy coming up the walk. She opened the front door. The deputy told her: “I have an arrest warrant for your son.” “Why, what did he do?” asked the mother. The deputy explained that her son had failed to show up in court a few months earlier on a traffic ticket. The mother responded: “but he’s been serving in Iraq for three years!”

It turned out that one of her son’s friends, himself facing arrest on a warrant in a different county, used her son’s name and birth date to get out of a traffic stop without being taken into custody. Of course, he failed to appear in court and a bench warrant was issued.

The young soldier’s mother recognized that this appropriation of her son’s identity created a criminal justice system record that could come back to haunt him. She was concerned that he might face unfair loss of job or housing opportunities upon his return from military service. At the sheriff’s suggestion she contacted Minnesota’s Bureau of Criminal Apprehension (BCA) in St. Paul, Minnesota and asked that the mistaken record be corrected. The BCA was able to help—but only to a point. The agency could make the appropriate annotations in its own database but had no control over data in the hands of commercial data miners.² It is a common

² E-mail from Timothy J. O’Malley, Superintendent, Minn. Bureau of
problem: creators of data have little ability to control its secondary or “downstream” uses, especially on the Internet.

This downstream-data problem occurs with such frequency that the BCA has a standard form letter that it gives to identity theft victims like the young soldier. It reads, in part:

We have performed a criminal history check based on the above referenced name and date of birth. This name and date of birth appear on a criminal history record. A fingerprint comparison has determined the holder of this letter is not the subject of that record. 

The BCA’s “questioned identity” letter could be helpful for those job or lease applicants who have an opportunity to respond to the contents of a background check report. However, due to the easy availability of unregulated “discreet” background checking services on the Internet, an applicant can remain entirely in the dark about what the record shows, unable to clear up mistakes.

For example, consider how in the following scenario the soldier could face an unfair outcome caused by a well-intentioned, conscientious person using legally-obtained background check...
data:

A landlord screening apartment lease applications sees that her first applicant, the young soldier, has a criminal justice system record. Wishing to protect her other tenants from someone who may have been involved in criminal behavior, she moves to the second application in the file. The second applicant shows no criminal history at all. She returns the second applicant’s call, and he ends up renting the apartment.

The property owner in this scenario could make decisions quickly, thanks to an almost unlimited availability of unregulated commercial background checking services on the Internet. But she made decisions without knowing she had only partial information, unaware that the first applicant is a law-abiding person whose record exists only because of a mistake.

The young soldier, like everyone in America, has a fundamental right of privacy that protects him from government intrusion. He should be able to come back from Iraq and live a quiet, private life uninterrupted by the influence of a government database. His privacy interests are in tension with the public’s right to know. When government transparency and perceptions of public safety conflict with individual privacy rights, privacy tends not to prevail despite the unintended consequences suffered by people like the young soldier.

An additional level of unintended result is introduced by the fact that criminal histories are not uniformly available. The second applicant in the apartment rental scenario could have had a felony conviction, but if it occurred in a county with a small tax base and historical records on paper rather than an electronic database, it is not so easily collected by data miners and therefore may be unavailable to the background checking service used by the property owner. The convenience of rapidly provided information on the Internet, coupled with the provider’s marketing disincentive to disclose its incompleteness, could result in the property owner passing up a law abiding person and instead renting to the

5. This article examines effects of unregulated harvesting and selling of government data on the Internet. The reader should be aware that the unregulated business model is in competition with reputable online background checking services that operate within the restrictions imposed upon them by federal and state law.

A convicted felon. In such a case, spotty data availability creates government opacity and allows the convicted felon an inadvertent measure of privacy.

A wide continuum occupies the space between privacy rights and the need for government transparency. This continuum is at the core of any discussion about how widely criminal justice data should be spread. At the privacy end of the continuum, the young soldier has the right to be left alone. At the transparency end, we want government records of felony convictions to be public. Along the middle of the continuum lay more difficult questions, such as:

- Should someone arrested but not charged have this fact available to potential employers?
- Should someone who broke the law as a child have their record follow them into adulthood?
- Should someone who has paid their debt to society and worked hard to become rehabilitated be given the chance for a fresh start?

Though privacy rights exist along a continuum, Internet data availability does not. There are no grey areas; it is a binary world. Once data are online, they are there for everyone, and they are there for all time. Even though a record may be removed by its originator, there is no ability to control who has copied it, and who may make the record reappear. No court has the world-wide jurisdiction that would be necessary to regulate the World Wide Web.

With the arrival of ubiquitously-available government data from myriad sources on the Internet combined with a generally elevated level of fear and mistrust in the post-9/11 decade, it is clear that the balance between privacy and transparency has shifted toward making more data available, not less. We are afraid of bad guys and we expect government technology to protect us from them. We tend to believe what we read online, and it is in our nature to presume guilt.

7. See Jerome E. Carlin, Jan Howard & Sheldon L. Messinger, Civil Justice and the Poor 74 (Russell Sage Foundation 1967) (noting the temptation of “overworked” judges to presume guilt in a civil setting). Overworked people screening job or rental applications are subject to the same tendency. See Neil Vidmar, Generic Prejudice and the Presumption of Guilt in Sex Abuse Trials, 21 LAW & HUM. BEHAV. 5, 6 (1997) (positing the existence of a “generic prejudice” driven by general attitudes, beliefs, and biases).
Before government technology made the criminal justice system’s records easily available, its data languished in what the Supreme Court termed “practical obscurity.”

Records technically were open to public inspection but practically inaccessible, tucked away in metal file cabinets or early, non-web-accessible databases. Only those who were patient enough to travel to the courthouse and wait on a wooden bench could view criminal justice system records. Compiling an individual’s statewide criminal justice data would take weeks; today, the same task is accomplished in seconds.

Practical obscurity helped ameliorate the criminal justice system’s harshness. Mistaken records existed, names and dates of birth were confused, but the obscurity of the record made it unlikely that errors would harm innocent people. Mistakes were correctable using a bottle of White-Out; today, the same sorts of mistakes are replicated endlessly on Internet-connected computers worldwide.

People arrested or charged with a crime but never convicted also benefited from practical obscurity’s mitigating effects. Large numbers of people—in some cases, a majority—arrested for low-level misdemeanors are either never charged or have their charge dismissed. When criminal justice records are posted online, these innocent people now feel the full measure of public record harshness. Those arrested but never convicted cannot easily move forward with their lives: their mug shots may appear on the local sheriff’s website within hours where they are easy pickings for commercial data miners.

9. As recently as 1990, criminal cases in Minnesota’s second-most populous county were indexed by entering case names in longhand using a fountain pen and blue ink in a large, leather and canvas-bound ledger.
10. Robert Sykora, Our New Permanent Punishment Machine, COUNCIL ON CRIME AND JUSTICE, http://www.crimeandjustice.org/councilinfo.cfm?pID=65 (last visited Nov. 19, 2010) (citing statistics from Minnesota State Court Administrator’s Office that in 2004 almost sixty percent of misdemeanor charges resulted in dismissal or not guilty verdict in Minnesota’s two most urban counties: Hennepin and Ramsey); see also COUNCIL ON CRIME AND JUSTICE, LOW LEVEL OFFENSES IN MINNEAPOLIS: AN ANALYSIS OF ARRESTS AND THEIR OUTCOMES (2004), available at http://www.racialdisparity.org/files/LowLevelOffenseStudyFinal11.09.04.pdf (analyzing selected low-level misdemeanors and finding that only 21.9% of those arrested were convicted; further noting that blacks were fifteen times more likely than whites to be arrested or cited).
11. See, e.g., BUSTED, http://www.bustedpaper.com (last visited Nov. 19, 2010) (featuring “hundreds of mug shots of local people” who were arrested during the
the Internet, unproven accusations affect data subjects profoundly. Potential landlords and employers will regard them skeptically. Their personal relationships will suffer. Their futures will be compromised.

Repurposed and ubiquitously available data can have terrible unintended consequences. If we are to avoid further creating a world where absolution, forgiveness, rehabilitation, and redemption are impossible, we need to agree upon a solid set of principles to guide us.

Without adherence to a set of principles, we suffer consequences when imperfect government data are repurposed for commercial use via unregulated commercial data mining. Section II of this article explores these consequences and their primary cause: that is, problems inherent in the criminal justice system’s data-gathering processes.

Section III sets forth the Fair Practice Principles embodied in the Minnesota statutes. Section IV reviews the various ways state legislatures have attempted to regulate this process by applying Fair Information Practice Principles. Section V highlights the steps that Minnesota has taken and can take to apply these principles when criminal justice system data is used by commercial data harvesters.

II. IMPERFECT DATA IN, IMPERFECT DATA OUT

A. Government Technology is Infallible, Right?

Hollywood has messed up our expectations for the criminal justice system. On the popular television drama CSI, crime scene investigators routinely nab the perpetrator after processing a tiny snippet of evidence with some sort of beeping, blinking gizmo. Real-life juries’ expectations are shaped by CSI’s depictions of such rapid and precise outcomes; their expectations about the quality of evidence offered in criminal cases are inflated as a result.12

---

Frustrated real-life prosecutors lament this “CSI Effect.”

On an even larger scale, screenwriters have shaped our expectations about the accuracy and comprehensiveness of online databases. It is a staple of both small and large-screen dramas to feature a bright computer screen that, after the requisite number of beeps, locates the bad guy on a color map, usually within a blinking red box with crosshairs.

Such depictions of electronic certainty comfort us: we want to believe there is order in the universe, especially where bad guys are concerned. As with the CSI Effect, however, reality intrudes upon this hopeful fantasy. Given the imperfections inherent in the criminal justice system’s data gathering processes, it is simply impossible for any commercial data harvester to be able to promise to their customers that an online background check is entirely accurate, complete, and current. Data consumers’ Hollywood-inflated expectations collide with the reality of government data gathering capabilities.

B. Our Courts’ Reliance on Names and Dates of Birth to Identify Defendants: An Inexact Science

Spend a morning in any criminal arraignment courtroom and you will be shocked by its imprecision. To get the work done, everyone operates under severe time pressure. Records are incomplete. Names are confused. Birth dates are missing or numbers are transposed. When many people have very similar or identical names and dates of birth, database chaos results. Cultural and language barriers are one contributing factor. Consider the following two examples, the first having to do with birth date inaccuracy and the second relating to confusion about naming structure.

1. Birth Date Inaccuracy

When working with people who were born in Somalia where there is no functioning government, Minnesota court workers were at first perplexed to see that improbable numbers of people shared January 1 as their birthday. It did not take long to realize that no functioning government means no official records of birth, so immigrants

14. See, e.g., DATE NIGHT (20th Century Fox 2010) (wherein the Mark Wahlberg character utilizes such a blinking computerized locator).
had simply selected the first day of January and a plausible year as a rough estimate, perhaps to satisfy an impatient immigration clerk.\textsuperscript{15} Being unable to differentiate people by birth date creates confusion: Minnesota’s courts rely entirely upon name and date of birth to track cases dealing with low-level offenses (the vast bulk of work done in criminal courts);\textsuperscript{16} only when an offender has been convicted of a more serious offense is he assigned an identifying number that is linked to his fingerprint record.

2. Name Inaccuracy

Court and law enforcement data systems dependent upon name and date of birth for identification are further confounded by both common names and names that do not fit easily into First-Middle-Last structure.

The tradition in some societies is to give a few names to many people. Large numbers of people named in Islamic cultures share a few names of religious figures (e.g., Muhammad or Fatima).\textsuperscript{17} Similarly, almost a quarter of all Korean immigrants share the same last name.\textsuperscript{18}

In Hispanic cultures, naming structure is more elaborate than the American tradition, with first and middle names followed by the father’s last name, the mother’s last name, and (for married women) the husband’s father’s last name.\textsuperscript{19} When a woman is

\textsuperscript{15} See Ted Gest, The Cyber Rap Sheet, Governing, Sept. 2001, at 26 (discussing the misalignment between data users’ expectations and actual data comprehensiveness); see also Jan. 1 Birthday Confusion in Criminal System: Birth Date a Factor in Seward Market Murder Case (Fox9News television broadcast Feb. 23, 2010), http://www.mymnytwincities.com/dpp/news/birth-date-confusion-in-henn-co-criminal-system (suggesting that “[o]f the 80,000 refugees who resettled in the U.S. last year, nearly 11,000 have January 1 birthdays.”).


\textsuperscript{19} E-mail from Deborah R. Lemon, Professor of Spanish Language Instruction, Ohlone Coll., Freemont, CA, to Robert Sykora, Chief Info. Officer, Minn. Board of Pub. Defense (Sept. 15, 2010) (on file with author).
identified as Rosa María Muñoz Izquierdo de Gómez, and the hurried deputy sheriff or district court clerk is facing database screens with fields allowing only first, middle and last names, what is the optimal response? One clerk may record Rosa María Muñoz while the next clerk types in Rosa Muñoz Gómez. In addition to making it difficult to differentiate defendants, multiple names for one person in a criminal justice database can create an implication of bad character. Once Rosa’s criminal justice data are harvested by a commercial service and made available in web-based background checks, her name will appear with one or more Also Known As (AKA) indicators. Imagine a decision-maker faced with two applicants: one applicant has a web-based background check report using only one name, the other has multiple AKAs. It is reasonable to assume that in some circumstances the decision-maker concludes that anyone with aliases has been up to no good, and this uncertainty disadvantages the applicant with a Hispanic or other name that does not easily fit into database structure.

Also, no surprise here, people lie and make mistakes. Any criminal justice system is dependent by its nature upon information provided by people who have a strong motive to distort the truth or who, almost by definition, may not be the brightest bulbs in the chandelier.

Social security numbers, used somewhat problematically to identify people in banking and other transactions, are not consistently used in the criminal justice system. Accommodating this federally regulated identifier would demand data security precautions and enhanced business practices with implementation costs way beyond the current budgets of criminal justice system data gatherers. Fingerprints help and prints electronically gathered and analyzed have improved the system’s ability to identify people rapidly. But the vast majority of criminal cases are misdemeanors, and the system does not have the resources to fingerprint most accused misdemeanants.

20. See BUREAU OF CRIMINAL APPREHENSION, BCA TECHNICAL DOCUMENTATION: MINNESOTA GENERATION 3 LIVESCAN MANUAL, at 6-3 (Version 3.0 2009), https://bcaneextest.x.state.mn.us/resources/bcageneration3livescanmanual.pdf (last updated June 2009). Multiple aliases also result when compound names are shoehorned into databases designed to accommodate only simple names. Id. For example, deputy sheriffs doing bookings in Minnesota are instructed to record Jose Rodrigues-Gonzalez’s name in four ways: (1) Gonzales-Rodriguez, Jose, (2) Rodriguez-Gonzales, Jose, (3) Gonzales, Jose, and (4) Rodriguez, Jose. Id. at 6–3.
Minnesota’s only public repository of statewide criminal conviction data resides at the BCA. By statute, criminal conviction records are made public for fifteen years when tied to a valid set of fingerprints belonging to the data subject, and when specified linking identifiers are present and consistent between courts and law enforcement.\textsuperscript{21} The BCA conviction database does not include the vast bulk of criminal convictions handled by the system; that is, nontargeted misdemeanors.\textsuperscript{22} Understanding the booking, fingerprinting, and court routines used to collect this information will help the reader understand how these routines sometimes fail and cause missing and inaccurate data.

The process of gathering a valid fingerprint is not as simple as we might like to believe. As we have already pondered the CSI Effect and our related tendency to over-rely upon the accuracy of government data, this should be of no surprise. It is a tricky task to capture an accurate two dimensional record of swirling lines on a squishy semispherical surface. Cartographers have faced similar impediments as they attempt to map the sphere upon which we live: the Mercator, Peters, Mollweide, Eckert, Goode, Van der Grinten, Winkel Tripel, and Robinson global map projections each differently portray the same layout of lines on the surface of the Earth. Further, lines upon a fingertip distort when pressed against a flat surface and require a delicate touch called “ink and roll” (the traditional method of law enforcement fingerprint gathering).

Newer technologies generically referred to as “Livescan” allow inkless fingerprinting in jails but still require that the fingertip properly be rolled to record an acceptable image. In Minnesota’s county jails, Livescan is used in all but about one hundred of each month’s 13,000 bookings\textsuperscript{23}, increasing accuracy by detecting flawed prints much sooner in time than is possible with the ink-and-roll technique. In a jail booking scenario, this speedy response is essential: “sooner in time” means \textit{while the person is still under law}.

\begin{footnotesize}
\begin{enumerate}
\item MINN. STAT. § 13.87, subdiv. 1(b) (2008 & Supp. 2010).
\item MINN. STAT. § 299C.10, subdiv. 1(e) (2008 & Supp. 2010) (providing that only misdemeanors listed in this statute are “targeted,” including the crimes of driving while impaired, order for protection violations, fifth-degree assault, domestic assault, interference with privacy, harassment or restraining order violations, and indecent exposure. All other misdemeanors are excluded from the BCA’s criminal history database.).
\item Telephone Interview with Jerrold Olson, AFIS Project Manager, Minn. Bureau of Criminal Apprehension (July 7, 2010) (providing “Fingerprint Services 2010” spreadsheet showing January–June 2010 statewide fingerprint serviced statistics) (on file with author).
\end{enumerate}
\end{footnotesize}
enforcement control and therefore available for re-fingerprinting to correct errors. Valid prints are rapidly compared with a database of known prints to help defeat identity theft schemes. With ink-and-roll prints, a flawed fingerprint card might eventually be detected by a fingerprint technician at the BCA, but likely not until weeks or months have elapsed and the suspect is no longer in the jail.

There is no doubt that Livescan has increased accuracy of Minnesota’s criminal justice system data. But even the most cutting-edge technologies are only as good as their operator. Consider this scenario: fingerprint examiners at the BCA tell the story of a deputy sheriff booking someone who was missing a ring finger. The Livescan device was not satisfied with nine prints, scolding the deputy with an error message. In a hurry to complete the booking before the end of his shift, the deputy obliged the complaining machine by substituting a scan of his own ring finger. The resulting defective fingerprint record would cause any related conviction to be kept out of the public criminal history record.24

While bloopers like this no doubt are a rare exception in an otherwise functional system of gathering fingerprints, the problem would not seem small to the employer or landlord making a decision based on the absence of a conviction record causing a felon amputee to appear as pure as the driven snow.

Even if the fingerprinting process was flawless, a devious defendant still has the chance to pass himself off as someone else when standing before the judge. Minnesota’s court system has declined to install fingerprint readers in its courtrooms,25 perhaps wishing to avoid blurring the line between law enforcement and adjudication.

Impediments to accuracy are everywhere. Despite them, clerks and lawyers with years of experience develop a knack for figuring out which records of misdeeds are relevant to the guy who is about to stand before the judge. After working with thousands of records, they know when something does not look right. They compare information from multiple databases: court records, sheriff jail booking records, the Department of Corrections, the Department of Driver and Vehicle Services, and the Bureau of Criminal Apprehension. They know that each database has its quirks and know how information from one can compensate for defects in

24. Id.
25. Id.
another. They are good at their work. Justice is done more often than not.

It is foolish to extract only the raw data from this process, to leave all the expertise behind, and to make the information available for anyone to use when making decisions about others’ lives.

C. Our Ability to Move Data Rapidly Has Outpaced Our Ability to Understand It

Criminal case records are easily available for a lot of good reasons—transparency and accountability being at the top of the list. Commercial data miners have scooped up this free, public government data for years. They repackage the information and make it available on the Internet for their customers.26 Technological advances over the past decade have been astounding, allowing quick, cost-effective data mining and rapid, easy searching of databases that are available to anyone at low cost. But the ability to obtain data does not guarantee the ability to understand it.

It is fair to surmise that the average data consumer’s ability to interpret criminal justice system data has not advanced as rapidly as has the technology used to disseminate that data. When is the nature of a government record sufficiently severe to justify disqualifying an applicant? A petty misdemeanor parking ticket? Just an arrest with no conviction? A guilty plea with a continuance for dismissal? A conviction that has been expunged by a judge? Only a rudimentary understanding of human nature is needed to find the answer to this question. People tend to believe that when there’s smoke, there’s fire.

When an online background check produces even a small suggestion of wrongdoing, it is human nature to take the safest possible course of action and move on to the applicant who appears to be free of wrongdoing. Why? Because of a natural fear of bad guys, because of a fear of civil liability, and because of the deeply ingrained tendency to presume guilt.27

26. For examples of “discreet” and “confidential” background checking services, see DELIVERY TEAM REPORT, supra note 4.
27. Vidmar, supra note 7. But see Louis Katzner, Presumptions of Reason and Presumptions of Justice, 70 J. PHILOS. 89, 89–100 (1973) (arguing that neither the presumption of innocence nor the presumption of guilt is necessarily a rational response).
D. Where There’s Smoke, There’s Guilt

We all presume guilt. It is natural. Even after a quarter-century as a public defender, when I drive by a guy on the shoulder of a road who is spread-eagled on the hood of a squad car I tend not to think, “that poor innocent is being unduly harassed!” and instead wonder, “what did he do?”

There is a pretty good argument that the presumption of guilt has served us well evolutionarily. If you assume that a shadow in the woods belongs to a cuddly friend, you increase the risk of being eaten. Always assume it is a predator and you increase the chance that you will spread your genetic material to a subsequent generation.

Today’s uncertainties are less often shadows in the woods than they are shadows in electronic data. When you perform a web-based background check and see information that is incomplete or imprecise, you may have no way to be certain that the record really belongs to the person you are checking. There is no way you can rule it out, either. The natural tendency in response to this uncertainty is to indulge the impulse that has served your genetic line so well over the millennia: that is, to conclude that a threat lurks within the shadows of the electronic record.

Decision-making of this sort has its downside both for the applicants and the decision-maker. The most obvious disadvantage is suffered by the applicant who has done nothing wrong but whose record is in some way muddled or confused with someone else’s. This applicant is also hurt by the off-the-record nature of the online investigation: he may never get a phone call; he may receive only a form rejection letter, and, therefore, he may never know that an employment or housing rejection was based on erroneous, incomplete, or improperly-disseminated online data. It has always been common for public defenders to hear from their clients, “I don’t know why I can’t get a job! I apply over and over but I never get a call!”

28. See Richard Dawkins, The Selfish Gene 59–63 (1976) (arguing that as the “survival machines” for our genes, we are programmed to respond to uncertainty by choosing the path we think least likely to involve risk).

29. Id.

30. See, e.g., Lora Pabst, Fresh Start Blocked by Court Error, Star Trib. (Minneapolis), Sept. 27, 2010, available at http://www.startribune.com/local/103762199.html?sl=KArksUUYUycaEacyU (describing a young man whose juvenile record was mistakenly posted on the Internet by the Minnesota court
housing contribute to a self-stoking cycle of poverty, defeat, criminal behavior, and repeated status as a public defender client.

A less obvious flaw affects those who make decisions based on online data harvested from the criminal justice system. Because of the data’s inherent flaws, it is entirely possible that the applicant who appears online to be “pure,” in fact has a felony conviction unreported for any of a wide variety of causes. As powerful an instinct as the presumption of guilt may be, it is thwarted when the decision-maker relies on bad and missing data.

When we recognize how the presumption of guilt is such a deep and natural impulse, it is easy to appreciate the wisdom inherent in the Bill of Rights as it creates the artificial courtroom environment where the opposite presumption is mandated. As we ponder a commonsense data policy, it is important to recognize that the Bill of Rights does not mandate the same difficult presumption in the daily conduct of our lives and in our business decisions.

E. Openness in Government Meets the Internet

Minnesota is famous for its lovely lakes, its dreadful winters, and the openness of its government data. This openness is driven by the Minnesota Government Data Practices Act (MGDPA), the nation’s premier model of government-in-the-sunshine legislation.31 Conceived in the post-Watergate era as a response to government secrecy abuses including Watergate, the MGDPA was the first data privacy statute in the nation.32 It created an admirable “come and get it” presumption; that is, government records belong to the people and therefore are presumed to be publicly accessible unless specifically excepted by statute.33 The MGDPA opened countless government file cabinets to public inspection.

32. Donald A. Gemberling & Gary A. Weissman, Everything You Wanted to Know About the Data Practices Act, From A to Z, 8 WM. MITCHELL L. REV. 573, 574 (1982).
Since the MGDPA was conceived in the early 1970s, file cabinets have become a quaint anachronism and the meaning of public data has expanded to describe information that is available instantaneously, globally, and irretrievably on the Internet. While the MGDPA presciently was written in a way that applies equally to both paper and electronic records, MGDPA authors could not have anticipated the consequences of ubiquitously available criminal justice system data.

Significant public policy implications are created when such a level of openness is applied to criminal justice system records. At least forty states—none with a tradition of openness in government records as robust as Minnesota’s—have responded to these public policy concerns by crafting legislative solutions directed at limiting the use of criminal justice data and increasing its quality. Given the international and virtual environment created by the Internet, no approach seen so far is a “slam dunk” solution.

III. THE NEED FOR A SOLID SET OF STANDARDS TO GUIDE USE OF CRIMINAL JUSTICE SYSTEM DATA

Policymakers need to agree on a solid set of principles to guide the repurposing of criminal justice system data by the Internet background-checking process. Fortunately, we need not invent a new set of principles. The Fair Information Practice Principles (often called simply “the FIPPs”) are internationally recognized and respected, having been at the core of international, national, and Minnesota data policy for about forty years. The Organization for Economic Cooperation and Development, the Federal Trade Commission, and Minnesota law have embraced the FIPPs as being at the core of a shared understanding of fair play and justice when making decisions about information use.

34. See, e.g., Minn. Stat. § 13.02, subdiv. 7 (2008) (creating a definition of government data not dependent upon “its physical form, storage media or conditions of use”).


principles were formed in the early 1970s when the U.S. Department of Health, Education and Welfare studied the effects of data gathering and the need for guiding principles.  

Four of these principles embodied in Minnesota law are especially relevant to the new world where commercial data harvesters make criminal justice data available on the Internet:

1. **Transparency:** There must be a way for the data subject to find out what information is in a record about her/him and how it is used.  

2. **Opportunity to correct:** There must be a way for a data subject to correct or amend a record of identifiable information about her/him.  

3. **Assure reliability:** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.  

4. **Control of use:** There must be a way for a person to prevent information about her/him that was obtained for one purpose from being used or made available for other purposes without consent.

These four foundational fairness principles provide an analytical framework for the next section of this article.

---

IV. STATE LEGISLATURES’ ATTEMPTS TO APPLY FAIR INFORMATION PRINCIPLES

Commercial data harvesting of criminal justice system records is an enterprise that involves coordinated effort among multiple actors with varying degrees of accountability to regulation. Some actors are regulated by U.S. federal law, others by state statute, others by court rule, and still others—by virtue of the multijurisdictional and difficult-to-trace nature of Internet transactions—are effectively accountable to no one. State legislatures have, with varying degrees of success, tried to design solutions that apply the FIPPs to the Internet-based transactions that otherwise slip through the cracks of existing law.

A. The Transparency Principle in State and Local Regulation

The words “secret dossier” conjure up images of disturbing government abuses: consider the methods used to pursue purported Communist sympathizers by Senator Joe McCarthy and J. Edgar Hoover in the 1950s and Richard Nixon’s enemies list in the late 1960s. It is no wonder that the FIPPs emerged in the 1970s with transparency as a central theme. Holding data practices true to the transparency principle helps avoid secret dossiers and enables data subjects to find inaccurate data and seek its correction.

The MGDPA creates a model of “passive transparency,” requiring government agencies to respond when data subjects ask to see statutorily accessible information. This transparency allowed the mother of the young soldier in the scenario at the beginning of this article to learn how her son had been victimized.

42. See Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (2008) (regulating circumstances where adverse action is taken in response to a consumer report prepared by a consumer reporting agency). Each of these underlined terms has a highly specific definition within the FCRA; transactions not consistent with these multiple definitions are not regulated by FCRA. See 15 U.S.C. § 1861a (2008). The authors note that this article focuses upon the effects of unregulated data miners using the Internet, not upon the services that conform to the FCRA.

43. See infra notes 51–52 and accompanying text.

44. See The Rules of Public Access to Record of the Judicial Branch (2005), available at http://www.mncourts.gov/rules/publicaccess/accessrules.pdf. The author notes that the focus of this article is on statutory comparison, not on court access to rules as they vary between states—such a task is important but is left to another author and another day.

by identity theft.

The cities of Minneapolis and St. Paul expand the transparency mandate in two ways: (1) the mandate is applied to the private sector, and (2) the city ordinances require active rather than passive transparency. In these two cities, landlords must disclose the criteria by which a potential tenant’s application will be judged, any criteria they failed to meet, and contact information for the background check service used to screen the applicant. While this process provides for the sort of transparency set forth in the FIPPs and provides data subjects with the information they need to pursue correction of data, this positive effect is not specifically intended: rather, the two City Councils put their ordinances in place to reduce opportunities for application fee-gouging by landlords.

46. Minneapolis’s ordinance states:
Licensing standards. The following minimum standards and conditions shall be met in order to hold a rental dwelling license under this article. Failure to comply with any of these standards and conditions shall be adequate grounds for the denial, refusal to renew, revocation, or suspension of a rental dwelling license or provisional license. (16)a. Before taking a rental application fee, a rental property owner must disclose to the applicant, in writing, the criteria on which the application will be judged. (16)c. If the applicant was charged an application fee and the rental property owner rejects the applicant, then the owner must, within fourteen (14) days, notify the tenant in writing of the reasons for rejection, including any criteria that the applicant failed to meet, and the name, address, and phone number of any tenant screening agency or other credit reporting agency used in considering the application.

47. St. Paul’s ordinance states:
Rental application fee requirements if the applicant was charged an application fee and the rental property owner rejects the applicant, then the owner must, within fourteen (14) days, notify the tenant in writing of the reasons for rejection, including any criteria that the applicant failed to meet, and the name, address, and phone number of any tenant screening agency or other credit reporting agency used in considering the application.
ST. PAUL, MINN., ORDINANCES § 54.03(c) (2010).


49. Interview with Gary Schiff, Council member, Minneapolis City Council (Aug. 13, 2010) (on file with author).
California also has an active transparency requirement imposed upon the private sector. The state law is intended to protect data subjects by requiring those who compile background reports to include information about the data source in the report, thereby enabling data subjects affected by data defects to contact the source and ask for correction. This requirement may allow effective regulation of those services which compile reports within California where they clearly are subject to the state law. However, data harvesters doing business in another country who send results to California consumers using the Internet are much less easily held accountable to the state law.

50. California’s statute states:
Matters of Public Record; Source; Reports for Employment Purposes. (a) Each investigative consumer reporting agency that collects . . . information concerning consumers which are matters of public record shall specify in any report containing public record information the source from which this information was obtained, including the particular court, if applicable, and the date that this information was initially reported or publicized. (b) A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles, collects, assembles, evaluates, reports, transmits, transfers, or communicates items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer’s ability to obtain employment shall in addition maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer’s ability to obtain employment is reported it is complete and up to date. For purposes of this paragraph, items of public record relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments shall be considered up to date if the current public record status of the item at the time of the report is reported.
CAL. CIV. CODE § 1786.28 (a)–(b) (2009).
Active transparency is required in Oregon and North Dakota, where the state laws require the state police agency to

51. Oregon’s statute states:
   Request for criminal records information by agency other than criminal justice agency.
   (1) When a person or agency, other than a criminal justice agency or a law enforcement agency pursuant to ORS 181.555 (2), requests from the Department of State Police criminal offender information regarding an individual, if the department’s compiled criminal offender information on the individual contains records of any conviction, or of any arrest less than one year old on which there has been no acquittal or dismissal, the department shall respond to the request as follows:
      (a) The department shall send prompt written notice of the request to the individual about whom the request has been made. The department shall address the notice to the individual’s last address known to the department and to the individual’s address, if any, supplied by the person making the request. However, the department has no obligation to insure that the addresses are current. The notice shall state that the department has received a request for information concerning the individual and shall identify the person or agency making the request. Notice to the individual about whom the request is made shall include:
         (A) A copy of all information to be supplied to the person or agency making the request; (B) Notice to the individual of the manner in which the individual may become informed of the procedures adopted under ORS 181.555 (3) for challenging inaccurate criminal offender information; and (C) Notice to the individual of the manner in which the individual may become informed of rights, if any, under Title VII of the Civil Rights Act of 1964, and notice that discrimination by an employer on the basis of arrest records alone may violate federal civil rights law and that the individual may obtain further information by contacting the Bureau of Labor and Industries.
      (b) Fourteen days after sending notice to the individual about whom the request is made, the department shall deliver to the person or agency making the request the following information if held regarding any convictions and any arrests less than one year old on which the records show no acquittal or dismissal: (A) Date of arrest. (B) Offense for which arrest was made. (C) Arresting agency. (D) Court of origin. (E) Disposition, including sentence imposed, date of parole if any and parole revocations if any.
      (c) The department shall deliver only the data authorized under paragraph (b) of this subsection.
      (d) The department shall inform the person or agency requesting the criminal offender information that the department’s response is being furnished only on the basis of similarity of names and description and that identification is not confirmed by fingerprints.


52. North Dakota’s statute states:
   Criminal history record information—Required disclosure of certain dissemination. If the bureau disseminates information under section 12-60-16.6, unless the request was accompanied by an authorization on forms prescribed by the bureau and signed by the record subject, the bureau shall mail notice of that dissemination to the record subject at the...
notify the data subject at his last known address whenever it provides data about the subject. Mandating such actions by a statewide police agency is just fine in those jurisdictions that prohibit secondary dissemination of government data, thereby making data consumers entirely dependent on the state police agency. In states like Minnesota where government records are given without restriction to unlimited numbers of data harvesters, the state police agency has no idea when, where, or in what form their data are being re-released and so are unable to provide any notice to the data subject. Mandating notice by internationally located data harvesters would suffer the same enforcement defect articulated in the previous paragraph.

B. The Opportunity-to-Correct Principle in State Regulation

The young soldier’s mother not only learned from the BCA that her son was the subject of a mistaken record due to identity theft, she was able to use the MGDPA to demand its correction—at least at the government data source. Information transparency means little without providing to the data subject opportunity to seek correction of mistaken and incomplete data. Minnesota law sets out procedures for an individual to ask for correction or completion of data and sets out the government agency’s obligation to respond.53 Once the source data are corrected, it makes sense to require the data source to provide notice of the correction to those who have received the bad data. Minnesota does not require this, but such requirements are in place in Arkansas,54 Illinois,55 New York,56 and Wyoming.57 Such a

54. The Arkansas statute, titled Right of Review and Challenge, provides that if an individual finds error in his or her criminal history stored by the state and the state acknowledges the error and corrects it:

Immediately after correction . . . the agency responsible for the criminal history information shall notify every agency or person known to have received the criminal history information within the previous one-year period and provide the agency or person with corrected criminal history information. . . . A person whose criminal history information has been corrected may ascertain the names of those agencies or individuals known to have received the previously incorrect criminal history information.

ARK. CODE. § 12-12-1013, subdiv. (c) (1)–(3) (2010).
55. The Illinois statute, titled Error Notification and Correction Procedure,
states:

It is the duty and responsibility of the Department to maintain accurate and complete criminal history record information and to correct or update such information after determination by audit, individual review and challenge procedures, or by other verifiable means, that it is incomplete or inaccurate. Except as may be required for a longer period of time by Illinois law, the Department shall notify a requester if a subsequent disposition of conviction or a subsequent modification of conviction information has been reported to the Department within 30 days of responding to the requester.

20 ILL. COMP. STAT. 2635/12 (2010).

56. This section of the New York statute deals with “[p]rocedures for criminal history information check requests by providers” and states:

A provider requesting a check of criminal history information pursuant to this section shall do so by completing a form established for such purpose by the authorized agency in consultation with the division. Such form shall include a sworn statement of the authorized person certifying that: (i) the person for whose criminal history information a check is requested is a subject individual for whom criminal history information is available by law; (ii) the specific duties which qualify the provider to request a check of criminal history information; (iii) the results of such criminal history information check will be used by the provider solely for purposes authorized by law; and (iv) the provider and its agents and employees are aware of and will abide by the confidentiality requirements and all other provisions of this article. . . . A provider authorized to request a criminal history information check pursuant to this section may inquire of a subject individual in the manner authorized by subdivision sixteen of section two hundred ninety-six of this chapter. Prior to requesting such information, a provider shall: (i) inform the subject individual in writing that the provider is authorized or, where applicable, required to request a check of his or her criminal history information and review the results of such check pursuant to this section; (ii) inform the subject individual that he or she has the right to obtain, review and seek correction of his or her criminal history information under regulations and procedures established by the division; (iii) obtain the signed, informed consent of the subject individual on a form supplied by the authorized agency which indicates that such person has: A. been informed of the right and procedures necessary to obtain, review and seek correction of his or her criminal history information; B. been informed of the reason for the request for his or her criminal history information; C. consented to such request for a report; and D. supplied on the form a current mailing or home address.

N.Y. EXEC. LAW § 845-b(3)(b)–(c) (McKinney 2010).

57. The Wyoming statute, titled Inspection, Deletion or Modification of Information, states:

An individual has the right to inspect all criminal history record information located within this state which refers to him. The record subject may apply to the district court for an order to purge, modify or supplement inaccurate or incomplete information. Notification of each deletion, amendment or supplementary notation shall be promptly disseminated to any person or agency which received a copy of the record in question during the previous twelve (12) month period as well
requirement cannot be effective when data miners provide “discreet” and “confidential” background checks because their service makes no record of the identity of the searcher or the parameters of the search.\textsuperscript{58}

\textbf{C. The Reliability Principle in State Regulation}

To be reliable, data must be accurate, complete, and current. In criminal justice data, currency is especially important—last month’s arrest could be this month’s dismissal or acquittal. Failure to include the most recent data would provide inaccurate information. In 2010, Minnesota implemented a statute that encourages data currency by both (1) requiring background check reports made in the state to bear the date that information was received from the source,\textsuperscript{59} and (2) requiring the information be updated within a month preceding the report.\textsuperscript{60} Other states have similar requirements encouraging up-to-date data, including California,\textsuperscript{61} North Carolina,\textsuperscript{62} Texas,\textsuperscript{63} and New Mexico.\textsuperscript{64} All of

\textsuperscript{58}. For examples, see \textsc{Delivery Team Report}, supra note 4.

\textsuperscript{59}. Minn. Stat. § 332.70, subdiv. 4 (2008) (“[A] business screening service that disseminates a criminal record must include the date when the record was collected and a notice that the information may include criminal records that have been expunged, sealed, or otherwise have become inaccessible to the public since that date.”).

\textsuperscript{60}. Minn. Stat. § 332.70, subdiv. 2 (“A business screening service must not disseminate a criminal record unless the record has been updated within the previous month.”).

\textsuperscript{61}. California’s statute, titled Matters of Public Record; Source; Reports for Employment Purposes, states:

Each investigative consumer reporting agency that collects . . . information concerning consumers which are matters of public record shall specify in any report containing public record information the source from which this information was obtained, including the particular court, if applicable, and the date that this information was initially reported or publicized. . . . A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles, collects, assembles, evaluates, reports, transmits, transfers, or communicates items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer’s ability to obtain employment shall in addition maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer’s ability to obtain employment is reported it is complete and up to date. For purposes of this paragraph, items of public record relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments shall be
these provisions have the potential to effectively regulate services operating within each state. However, exercising state jurisdiction over data services located in foreign jurisdictions would be an insurmountable struggle for an indigent person unable to retain the services of a lawyer.

More efficacious and politically palatable solutions have been put in place by various state legislatures. Many are aimed at increasing the likelihood that data provided by government are accurate, complete, and current. Arizona requires a biometric

considered up to date if the current public record status of the item at the time of the report is reported.

**Cal. Civ. Code § 1786.28 (a)–(b) (2009).**

62. North Carolina’s statute, titled Civil Liability for Dissemination of Certain Criminal History Information, states:

- Unless the entity is regulated by the federal Fair Credit Reporting Act . . . or the Gramm-Leach-Bliley Act, . . . a private entity described by subsection (a) of this section that is licensed to access a State agency’s criminal history record database may disseminate that information only if, within the 90-day period preceding the date of dissemination, the entity originally obtained the information or received the information as an updated record information to its database. The private entity must notify the State agency from which it receives the information of any other entity to which it subsequently provides a bulk extract of the information.


63. Texas’s statute, titled Duty of Private Entity to Update Criminal History Record Information; Civil Liability, states:

- A private entity that compiles and disseminates for compensation criminal history record information shall destroy and may not disseminate any info in the possession of the entity with respect to which it has received notice that: (1) an order of expunction has been issued under Article 55.02, Code of Criminal Procedure; or (2) an order of nondisclosure has been issued . . .

**Tex. Gov’t Code Ann. § 411.0851 (a) (2010).**

64. New Mexico’s statute, titled Report Information; Limitations, states:

- A credit bureau may report the following matters for no longer than the specified periods: . . . suits and judgments for not longer than seven years from date of entry, or until the governing statute of limitations has expired, whichever is the longer period; . . . arrests and indictments pending trial, or convictions of crimes, for not longer than seven years from date of release or parole. Such items shall no longer be reported if at any time it is learned that after a conviction a full pardon has been granted, or after an arrest or indictment a conviction did not result; and . . . any other data not otherwise specified in this section, for not longer than seven years. . . . A credit bureau shall delete as soon as practical any items of derogatory information whenever it is ascertained that the source of information can no longer verify the item in question from its records of original entry.

**N.M. Stat. Ann. § 56-3-6 (A) (3), (5)–(6), (B) (2010).**
match (in the form of fingerprints) before state records are released to noncriminal justice agencies.\textsuperscript{65} In North Dakota, the requestor can provide either fingerprints or additional identifying information and, in the fingerprint-less scenario, the state requires that the identifying information not match more than one individual (this would help protect a data subject from consequences of identity theft where a bad actor uses the victim’s name and identifying data to rack up criminal convictions in the victim’s name).\textsuperscript{66}

Finally, several states attempt to encourage reliability by discouraging staleness. They address data reliability concerns by prohibiting consumer reporting agencies from using arrests or

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{65} A R I Z. REV. STAT. ANN. § 41-1750 (G) (2) (2010) ("Each statute, ordinance, or executive order that authorizes noncriminal justice agencies to receive criminal history record information for these purposes . . . shall require that fingerprints of the specified individuals be submitted in conjunction with such requests for criminal history record information.").
\item \textsuperscript{66} North Dakota’s statute, titled Criminal History Record Information-Dissemination to Parties not Described in Section 12-60-16.5, states:
\begin{enumerate}
\item Only the bureau may disseminate a criminal history record to parties not described in section 12-60-16.5. The dissemination may be made only if all the following requirements are met:
\begin{enumerate}
\item The criminal history record information has not been purged or sealed.
\item The criminal history record information is of a conviction, including a conviction for violating section 12.1-20-03, 12.1-20-03.1, 12.1-20-04, 12.1-20-06.1, or 12.1-20-11 notwithstanding any disposition following a deferred imposition of sentence; or the criminal history record information is of a reportable event occurring within three years preceding the request.
\item The request is written and contains: a.) The name of the requester. b.) The fingerprints of the record subject or, if the request is made without submitting the fingerprints, the request must also include the name of the record subject and at least two items of information used by the bureau to retrieve criminal history records, including: (1) The state identification number assigned to the record subject by the bureau. (2) The social security number of the record subject. (3) The date of birth of the record subject. (4) A specific reportable event identified by date and either agency or court.
\item The identifying information supporting a request for a criminal history record does not match the record of more than one individual.
\end{enumerate}
\end{enumerate}
\end{itemize}

N. D. CENT. CODE § 12-60-16.6 (1)–(4) (2010).
\end{footnotesize}
convictions more than seven years old (California, Colorado, Kansas, Louisiana, Maine, Maryland, Massachusetts).

67. California’s statute, titled Items of Information Prohibited, states:

[A]n investigative consumer reporting agency may not make or furnish any investigative consumer report containing any of the following items of information [certain exceptions apply]: . . . Records of arrest, indictment, information, misdemeanor complaint, or conviction of a crime that, from the date of disposition, release, or parole, antedate the report by more than seven years.

CAL. CIV. CODE § 1786.18 (a) (7) (2010).

68. Colorado’s statute, titled Reporting of Information Prohibited, states:

[N]o consumer reporting agency shall make any consumer report containing any of the following items of information: . . . Suits and judgments that, from the date of entry, predate the report by more than seven years or by more than the governing statute of limitations, whichever is the longer period; . . . Records of arrest, indictment, or conviction of a crime that, from the date of disposition, release, or parole, predate the report by more than seven years; . . . Any other adverse item of information that predates the report by more than seven years.

COLO. REV. STAT. § 12-14.3-105.3 (1) (b), (e)–(f) (2010).

69. Kansas’s statute, titled Obsolete Information, states:

Except as authorized under subsection (b) of this section, no consumer reporting agency shall make any consumer report containing any of the following items of information: . . . suits and judgments which, from date of entry, antedate the report by more than seven (7) years or until the governing statute of limitations has expired, whichever is the longer period; . . . records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven (7) years; and . . . any other adverse item of information which antedates the report by more than seven (7) years.


70. Louisiana’s statute, titled Authority to Purge Records of the Central Repository, states:

Except for the provisions of R.S. 44:9, no records of the bureau may be permanently destroyed until five years after the person identified is known or reasonably believed to be dead. Upon the official issuance of appropriate rules and regulations, the bureau may retire or remove from active dissemination to eligible agencies records of any individual beyond the age of sixty, who has had no reported criminal arrest for a period of fifteen years from the last reported official release from the criminal justice system.


71. Maine’s statute, titled Requirements Relating to Information Contained in Consumer Reports, states:

Except as authorized under subsection 2, a consumer reporting agency may not make any consumer reports containing any of the following items of information: . . . Civil suits, civil judgments and records of arrest that, from date of entry, antedate the report by more than 7 years or until the governing statute of limitations has expired, whichever is the longer period; . . . Any other adverse item of information, other than records of conviction of crimes, that antedates the report by more than 7 years.
Montana, Nevada, New Hampshire, New Mexico, New York


72. Maryland’s statute, titled Information to be Excluded, states:
Except as authorized under subsection (b) of this section, no consumer reporting agency may make any consumer report containing any of the following items of information: . . . Suits and judgments which, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period; . . . Records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years; or . . . Any other adverse item of information which antedates the report by more than seven years.

MD. CODE ANN., COM. LAW § 14-1203(a)(2), (5)–(6) (West 2010).

73. Massachusetts’ statute, titled Information not to be Contained in Report;
Exceptions, states:
Except as authorized under subsection (b) no consumer reporting agency shall make any consumer report containing any of the following items of information: . . . suits and judgments which, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired. . . . Records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years. Any other adverse item of information which antedates the report by more than seven years.

MASS. GEN. LAWS ch. 93, § 52(a)(2), (5)–(6) (2010).

74. Montana’s statute, titled Obsolete Information, states:
No consumer reporting agency may make any consumer report containing any of the following items of information: . . . suits and judgments which, from date of entry, antedate the report by more than 7 years or until the governing statute of limitations has expired, whichever is the longer period. . . . Records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than 7 years; . . . any other adverse item of information which antedates the report by more than 7 years.


75. Nevada’s statute states:
Purging of information from files of reporting agency; disclosure of purged information. A reporting agency shall periodically purge from its files and after purging shall not disclose: . . . 2. Except as otherwise provided by a specific statute, any other civil judgment, a report of criminal proceedings, or other adverse information which precedes the report by more than 7 years.


76. New Hampshire’s statute states:
Except as authorized under paragraph II, no consumer reporting agency may make any consumer report containing any of the following items of information: . . . (e) Records of arrest, indictment, or conviction of crime which, from date of disposition, release, or parole, antedate the report by more than 7 years; (f) Any other adverse item of information which antedates the report by more than 7 years.


77. New Mexico’s statute states:
A credit bureau may report the following matters for no longer than the specified periods: . . . (3) suits and judgments for not longer than seven years from date of entry, or until the governing statute of limitations has expired, whichever is the longer period; . . . (5) arrests and indictments pending trial, or convictions of crimes, for not longer than seven years from date of release or parole. Such items shall no longer be reported if at any time it is learned that after a conviction a full pardon has been granted, or after an arrest or indictment a conviction did not result; and (6) any other data not otherwise specified in this section, for not longer than seven years.

B. A credit bureau shall delete as soon as practical any items of derogatory information whenever it is ascertained that the source of information can no longer verify the item in question from its records of original entry.

N.M. STAT. ANN. § 56-3-6(A)(3), (A)(5)–(6), (B) (2003).

New York’s statute states:

(e) Consumer reporting agencies shall maintain reasonable procedures designed to assure maximum possible accuracy of the information concerning the individual about whom the report relates. (f)(1) Except as authorized under paragraph two of this subdivision, no consumer reporting agency may make any consumer report containing any of the following items of information. . . . (ii) judgments which, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period; or judgments which, from date of entry, having been satisfied within a five year period from such entry date, shall be removed from the report five years after such entry date; . . . (v) records of conviction of crime which, from date of disposition, release, or parole, antedate the report by more than seven years; . . . (viii) any other adverse information which antedates the report by more than seven years.


Pennsylvania’s statute states:

(b) Dissemination to noncriminal justice agencies and individuals.—Criminal history record information shall be disseminated by a State or local police department to any individual or noncriminal justice agency only upon request. . . . (2) Before a State or local police department disseminates criminal history record information to an individual or noncriminal justice agency, it shall extract from the record all notations of arrests, indictments or other information relating to the initiation of criminal proceedings where: (i) three years have elapsed from the date of arrest; (ii) no conviction has occurred; and (iii) no proceedings are pending seeking a conviction. . . . (f) Notations on record.—Repositories must enter as a permanent part of an individual’s criminal history record information file, a listing of all persons and agencies to whom they have disseminated that particular criminal history record information and the date and purpose for which the information was disseminated. Such listing shall be maintained separate from the record itself.


Texas’s statute states:

(a) Except as provided by Subsection (b), a consumer reporting agency
considers a matter to have gone stale after three years, and, if other
conditions are met, it cannot be disseminated.  

may not furnish a consumer report containing information related to: . . .
(2) a suit or judgment in which the date of entry predates the
consumer report by more than seven years or the governing statute of
limitations, whichever is longer; . . . (4) a record of arrest, indictment, or
conviction of a crime in which the date of disposition, release, or parole
predates the consumer report by more than seven years . . . .

TEX. BUS. & COM. CODE ANN. § 20.05(a)(2), (4) (West 2009).

Washington’s statute states:
(1) Except as authorized under subsection (2) of this section, no
consumer reporting agency may make a consumer report containing any
of the following items of information: . . . (b) Suits and judgments that,
from date of entry, antedate the report by more than seven years or until
the governing statute of limitations has expired, whichever is the longer
period . . . .


North Dakota’s statute states:
Only the bureau may disseminate a criminal history record to parties not
described in section 12–60–16.5. The dissemination may be made only if
all the following requirements are met:
1. The criminal history record information has not been purged or
sealed.
2. The criminal history record information is of a conviction, including a
conviction for violating section 12.1-20-03, 12.1-20-03.1, 12.1-20-04, 12.1-
20-06.1, or 12.1-20-11 notwithstanding any disposition following a
defered imposition of sentence; or the criminal history record
information is of a reportable event occurring within three years
preceding the request.
3. The request is written and contains:
   a. The name of the requester.
   b. The fingerprints of the record subject or, if the request is made
      without submitting the fingerprints, the request must also include the
      name of the record subject and at least two items of information used by
      the bureau to retrieve criminal history records, including:
         (1) The state identification number assigned to the record
         subject by the bureau.
         (2) The social security number of the record subject.
         (3) The date of birth of the record subject.
         (4) A specific reportable event identified by date and either
         agency or court.
4. The identifying information supporting a request for a criminal
history record does not match the record of more than one individual.
In order to confirm a record match, the bureau may contact the
requester to collect additional information if a request contains an item
of information that appears to be inaccurate or incomplete. This section
does not prohibit the disclosure of a criminal history record by the
requester or other persons after the dissemination of the record by the
bureau to the requester.

The young soldier in the scenario at the beginning of this article was damaged by data that were unreliable because a police officer was fooled by a lie, a problem that may better be addressed by changes to police procedure and equipment rather than data policy. 83

D. Control-of-Use Principle in State Regulation

1. Prohibiting Use of Non-Conviction Arrest Records for Other Purposes

Fair Information Practice Principles require that information collected by the government for one purpose cannot be used for another without the data subject’s consent. In its narrowest reading, this would mean that data collected about a criminal conviction could not be used by an employer making a hiring decision. Data subject consent is required before conviction data can be released to third parties in the states of Illinois, 84 New Jersey, 85 Virginia, 86 and Wyoming. 87 West Virginia requires consent


84. Illinois’s statute states:

(A) The following provisions shall apply to requests submitted pursuant to this Act for employment or licensing purposes or submitted to comply with the provisions of subsection (B) of this Section: (1) A requester shall, in the form and manner prescribed by the Department, submit a request to the Department, and maintain on file for at least 2 years a release signed by the individual to whom the information request pertains. The Department shall furnish the requester with a copy of its response. (2) Each requester of conviction information furnished by the Department shall provide the individual named in the request with a copy of the response furnished by the Department. Within 7 working days of receipt of such copy, the individual shall have the obligation and responsibility to notify the requester if the information is inaccurate or incomplete.

20 ILL. COMP. STAT. ANN. 2635/7(A)(1)-(2) (West 2008).

85. New Jersey’s statute states:

An applicant for employment or a current employee shall submit to the Commissioner of Human Services his name, address and fingerprints taken on standard fingerprint cards by a State or municipal law enforcement agency. . . . No criminal history record check shall be performed pursuant to this act unless the applicant shall have furnished his written consent to the check.

N.J. STAT. ANN. § 30:4-36 (West 2008).
for release of “records” as well as identifying data.\footnote{88}

Several states have designed approaches that seem to be the result of balancing the fairness principle with the idea that a person convicted of a crime should sacrifice at least some of his right to privacy. With this approach, records of conviction are able to be used, but criminal records not leading to conviction (or after exoneration) are restricted. This approach seems designed to avoid unfairly branding as “criminal” those people whose behavior cannot legally be labeled as such. The goal of protecting people who are presumed innocent from unpredictable, “shifting use” consequences is consistent with the philosophy of the Minnesota Supreme Court as expressed in its own Rules of Public Access to Records of the Judicial Branch. These rules prohibit “preconviction” data from being made available on the court web site.\footnote{89} The restriction applies only to judicial branch records;

\footnote{86. Virginia’s statute states:}
[U]pon a written request sworn to before an officer authorized to take acknowledgments, the Central Criminal Records Exchange, or the criminal justice agency in cases of offenses not required to be reported to the Exchange, shall furnish a copy of conviction data covering the person named in the request to the person making the request; however, such person on whom the data is being obtained shall consent in writing, under oath, to the making of such request.


\footnote{87. Wyoming’s statute states:}
Notwithstanding subsection (a) of this section, the division may disseminate criminal history record information concerning a record subject, or may confirm that no criminal history record information exists relating to a named individual: (i) In conjunction with state or national criminal history record information check . . . ; or (ii) If application is made for a voluntary record information check, provided: (A) The applicant submits proof satisfactory to the division that the individual whose record is being checked consents to the release of the information to the applicant . . . .


\footnote{88. West Virginia's statute states:}
The criminal identification bureau may furnish, with the approval of the superintendent, fingerprints, photographs, records or other information to any private or public agency, person, firm, association, corporation or other organization, . . . but all requests under th[is] provision . . . for such fingerprints, photographs, records or other information must be accompanied by a written authorization signed and acknowledged by the person whose fingerprints, photographs, records or other information is to be released.


\footnote{89. THE RULES OF PUBLIC ACCESS TO RECORDS OF THE JUDICIAL BRANCH, supra note 44, at 14, subdiv. 2(c).}
however, without a similar statutory restriction in place, police and sheriff agencies in Minnesota’s executive branch are free to disseminate information about unproven accusations.

The following states do have statutory restrictions on disseminating information about unproven criminal accusations: Arkansas, \(^90\) California, \(^91\) Connecticut, \(^92\) Georgia, \(^93\) Iowa, \(^94\) Kentucky. \(^95\)

\(^90\) ARK. CODE ANN. § 12-12-1009(c) (2009) ("Nonconviction information shall not be available under the provisions of this subchapter for noncriminal justice purposes.").

\(^91\) California’s statute states:

These items of information shall no longer be reported if at any time it is learned that, in the case of a conviction, a full pardon has been granted or, in the case of an arrest, indictment, information, or misdemeanor complaint, a conviction did not result; except that records of arrest, indictment, information, or misdemeanor complaints may be reported pending pronouncement of judgment on the particular subject matter of those records.


\(^92\) Connecticut’s statute states:

Nonconviction information other than erased information may be disclosed only to: (1) Criminal justice agencies in this and other states and the federal government; (2) agencies and persons which require such information to implement a statute or executive order that expressly refers to criminal conduct; (3) agencies or persons authorized by a court order, statute or decisional law to receive criminal history record information.Whenever a person or agency receiving a request for nonconviction information is in doubt about the authority of the requesting agency to receive such information, the request shall be referred to the State Police Bureau of Investigation. (a) Nonconviction information disseminated to noncriminal justice agencies shall be used by such agencies only for the purpose for which it was given and shall not be redisseminated.

CONN. GEN. STAT. ANN. § 54-142(n)–(o) (West 2009).

\(^93\) See GA. CODE ANN. § 35-3-34(a)(1)(B) (2006) ("The center may not provide records of arrests, charges, and sentences for crimes relating to first offenders . . . in cases where offenders have been exonerated and discharged without court adjudications of guilt . . . "); GA. CODE ANN. § 42-8-62(a) (Supp. 2010). Section 42-8-62(a) of the Georgia Code states:

Upon fulfillment of the terms of probation, upon release by the court prior to the termination of the period thereof, or upon release from confinement, the defendant shall be discharged without court adjudication of guilt. . . . [T]he discharge shall completely exonerate the defendant of any criminal purpose and shall not affect any of his or her civil rights or liberties; and the defendant shall not be considered to have a criminal conviction. It shall be the duty of the clerk of court to enter on the criminal docket and all other records of the court pertaining thereto the following: ‘Discharge filed completely exonerates the defendant of any criminal purpose and shall not affect any of his or her civil rights or liberties, except for registration requirements under the state sexual offender registry and except with regard to employment
Louisiana, Maine, Massachusetts, Nebraska, New York

providing care for minor children or elderly persons . . .; and the defendant shall not be considered to have a criminal conviction . . . .'

94. IOWA CODE ANN. § 692.17(1) (West Supp. 2010) ("Criminal history data in a computer data storage system shall not include arrest or disposition data or custody or adjudication data after the person has been acquitted or the charges dismissed . . . .").

95. Kentucky’s administrative regulations states:

Dissemination of nonconviction data shall, with the exception of the computerized Kentucky State Police files accessed by an open record request directly to the Department of State Police, be limited, whether directly or through an intermediary, to: (a) Criminal justice agencies for purposes of the administration of criminal justice and criminal justice agency employment. (b) Individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court order, as determined by the General Counsel, Justice Cabinet. (c) Individuals and agencies pursuant to a specific agreement . . . with the Department of State Police, to provide services required for the administration of criminal justice pursuant to that agreement. (d) Individuals and agencies for the express purpose of evaluation research, or statistical activities pursuant to an agreement with the Criminal Identification and Records Branch of the Kentucky State Police.

502 KY. ADMIN. REGS. 30:060(1)(a)–(d) (2010).

96. Louisiana’s statute provides:

C. Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to another criminal justice agency . . . .

D. . . . to implement a statute, ordinance, executive order, or a court rule, decision, or order which expressly refers to records of arrest, charges, or allegations of criminal conduct or other nonconviction data and authorizes or directs that it be available or accessible for a specific purpose.

E. Criminal history record information which includes nonconviction data may be disseminated to individuals and agencies pursuant to a contract with a criminal justice agency to provide services related to the administration of criminal justice. Such contract must specifically authorize access to criminal history record information, but need not specifically state that access to nonconviction data is included. The agreement must limit the use of the criminal history record information to stated purposes and insure the confidentiality and security of the information consistent with state law and any applicable federal statutes and regulations.

F. . . . for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. Such agreement must authorize the access to nonconviction data, limit the use of that information which identifies specific individuals to research, evaluative, or statistical purposes, and contain provisions giving notice to the person or organization to which the records are disseminated that the use of information obtained therefrom and further dissemination of such information are subject to this Chapter and applicable federal statutes and regulations, which shall be cited with express reference to the penalties provided for a violation thereof.

97. Maine’s statute provides:

Except as provided in section 612, subsections 2 and 3, dissemination of nonconviction data by a criminal justice agency, whether directly or through any intermediary, shall be limited to:
1. Criminal justice agencies . . . for the purpose of the administration of criminal justice and criminal justice agency employment;
2. Under express authorization. [e.g. authorized by statute, executive order, court rule, court decision or court order];
3. Under specific agreements. Any person with a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice or to conduct investigations determining the employment suitability of prospective law enforcement officers . . . .


98. Massachusetts’ statute states:

9. For an employer, himself or through his agent, in connection with an application for employment, or the terms, conditions, or privileges of employment, or the transfer, promotion, bonding, or discharge of any person, or in any other matter relating to the employment of any person, to request any information, to make or keep a record of such information, to use any form of application or application blank which requests such information, or to exclude, limit or otherwise discriminate against any person by reason of his or her failure to furnish such information through a written application or oral inquiry or otherwise regarding: (i) an arrest, detention, or disposition regarding any violation of law in which no conviction resulted, or (ii) a first conviction for any of the following misdemeanors: drunkenness, simple assault, speeding, minor traffic violations, affray, or disturbance of the peace, or (iii) any conviction of a misdemeanor where the date of such conviction or the completion of any period of incarceration resulting therefrom, whichever date is later, occurred five or more years prior to the date of such application for employment or such request for information, unless such person has been convicted of any offense within five years immediately preceding the date of such application for employment or such request for information.

MASS. GEN. LAWS ANN. ch. 151B, § 4, subdiv. 9 (West 2004).

99. Nebraska’s statute provides:

(1) That part of criminal history record information consisting of a notation of an arrest, described in subsection (2) of this section, shall not be disseminated to persons other than criminal justice agencies after the expiration of the periods described in subsection (2) of this section except when the subject of the record:
(a) Is currently the subject of prosecution or correctional control as the result of a separate arrest;
(b) Is currently an announced candidate for or holder of public office;
(c) Has made a notarized request for the release of such record to a specific person; or
(d) Is kept unidentified, and the record is used for purposes of surveying or summarizing individual or collective law enforcement agency activity or practices, or the dissemination is requested consisting only of release of criminal history record information showing (i) dates of arrests, (ii)
reasons for arrests, and (iii) the nature of the dispositions including, but not limited to, reasons for not prosecuting the case or cases.

(2) Except as provided in subsection (1) of this section, the notation of arrest shall be removed from the public record as follows:

(a) In the case of an arrest for which no charges are filed as a result of the determination of the prosecuting attorney, the arrest shall not be part of the public record after one year from the date of arrest;

(b) In the case of an arrest for which charges are not filed as a result of a completed diversion, the arrest shall not be part of the public record after two years from the date of arrest; and

(c) In the case of an arrest for which charges are filed, but dismissed by the court on motion of the prosecuting attorney or as a result of a hearing not the subject of a pending appeal, the arrest shall not be part of the public record after three years from the date of arrest.

NEB. REV. STAT. § 29-3523, subdiv. 1–2 (LexisNexis 2009).

100. New York’s statute provides:

(a) No consumer reporting agency shall report or maintain in the file on a consumer, information:

(1) relative to an arrest or a criminal charge unless there has been a criminal conviction for such offense, or unless such charges are still pending . . . .


101. Oregon’s statute provides:

If the department holds no criminal offender information on an individual, or the department’s compiled criminal offender information on the individual consists only of nonconviction data, the department shall respond to a request under this section that the individual has no criminal record and shall release no further information.

OR. REV. STAT. § 181.560(2) (West 2007).

102. Rhode Island’s statute provides:

(a) Any fingerprint, photograph, physical measurements, or other record of identification, heretofore or hereafter taken by or under the direction of the attorney general, the superintendent of state police, the member or members of the police department of any city or town or any other officer authorized by this chapter to take them, of a person under arrest, prior to the final conviction of the person for the offense then charged, shall be destroyed by all offices or departments having the custody or possession within sixty (60) days after there has been an acquittal, dismissal, no true bill, no information, or the person has been otherwise exonerated from the offense with which he or she is charged, and the clerk of court where the exoneration has taken place shall . . . place under seal all records of the person in the case, including all records of the division of criminal identification . . . provided, that the person shall not have been previously convicted of any felony offense . . . .

(b) The requirements of this section shall also apply to persons detained by police, but not arrested or charged with an offense, or to persons against whom charges have been filed by the court, and the period of such filing has expired.

R.I. GEN. LAWS § 12-1-12, subdiv. (a)–(b) (2002).

103. South Carolina’s statute provides:

A person who after being charged with a criminal offense and the charge
is discharged, proceedings against the person are dismissed, or the person is found not guilty of the charge, the arrest and booking record, files, mug shots, and fingerprints of the person must be destroyed and no evidence of the record pertaining to the charge may be retained by any municipal, county, or state law enforcement agency. Provided, however, that local and state detention and correctional facilities may retain booking records, identifying documentation and materials, and other institutional reports and files under seal, on all persons who have been processed, detained, or incarcerated, for a period not to exceed three years from the date of the expungement order to manage their statistical and professional information needs and, where necessary, to defend such facilities during litigation proceedings except when an action, complaint, or inquiry has been initiated. Information retained by a local or state detention or correctional facility as permitted under this section after an expungement order has been issued is not a public document and is exempt from disclosure. Such information only may be disclosed by judicial order, pursuant to a subpoena filed in a civil action, or as needed during litigation proceedings . . . .


104. Utah’s statute provides:

If an individual has no prior criminal convictions, criminal history record information contained in the division’s computerized criminal history files may not include arrest or disposition data concerning an individual who has been acquitted, the person’s charges dismissed, or when no complaint against the person has been filed.


105. Washington’s statute provides:

(3) Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to another criminal justice agency for any purpose associated with the administration of criminal justice, or in connection with the employment of the subject of the record by a criminal justice or juvenile justice agency . . . .

(4) Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to implement a statute, ordinance, executive order, or a court rule, decision, or order which expressly refers to records of arrest, charges, or allegations of criminal conduct or other nonconviction data and authorizes or directs that it be available or accessible for a specific purpose.

(5) Criminal history record information which includes nonconviction data may be disseminated to individuals and agencies pursuant to a contract with a criminal justice agency to provide services related to the administration of criminal justice.

(6) Criminal history record information which includes nonconviction data may be disseminated to individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency.

WASH. REV. CODE § 10.97.050(3)–(6) (West Supp. 2010).
2. **Controlling Downstream Use by Mandating “Data Babysitting”**

Of all the actors in the many arrangements that allow criminal justice data to be used by private entities, government employees are the easiest—but perhaps not the most effective—to regulate. Policymakers set limits that define proper handling of data: government agencies sign “permissible use” agreements, regular audits assess compliance, and sanctions follow when rules are transgressed.

While several state statutory schemes require that government employees release data only to noncriminal justice users who agree to use it properly (e.g., Arizona, Connecticut, Delaware)

106. The Arizona statute provides:

   (G) The director shall authorize the exchange of criminal justice information between the central state repository, or through the Arizona criminal justice information system, whether directly or through any intermediary, only as follows . . . .
   (2) With any noncriminal justice agency pursuant to a statute, ordinance or executive order that specifically authorizes the noncriminal justice agency to receive criminal history record information for the purpose of evaluating the fitness of current or prospective licensees, employees, contract employees or volunteers, on submission of the subject’s fingerprints and the prescribed fee. Each statute, ordinance, or executive order that authorizes noncriminal justice agencies to receive criminal history record information . . . .
   (Q)(3) Criminal history record information disseminated to noncriminal justice agencies or to individuals shall be used only for the purposes for which it was given. Secondary dissemination is prohibited unless otherwise authorized by law . . . .
   (6) Criminal history record information shall be released to noncriminal justice agencies of the federal government pursuant to the terms of the federal security clearance information act . . . .


107. Connecticut’s statute provides:

   Nonconviction information other than erased information may be disclosed only to: (1) Criminal justice agencies in this and other states and the federal government; (2) agencies and persons which require such information to implement a statute or executive order that expressly refers to criminal conduct; (3) agencies or persons authorized by a court order, statute or decisional law to receive criminal history record information. Whenever a person or agency receiving a request for nonconviction information is in doubt about the authority of the requesting agency to receive such information, the request shall be referred to the state police bureau of investigation.

   Conn. Gen. Stat. Ann. § 54-142(n)–(o) (West 2009). The statute further provides that “Nonconviction information disseminated to noncriminal justice agencies shall be used by such agencies only for the purpose for which it was given and shall not be redisseminated.” Id. at § 54-1520(a).

108. Delaware’s statute provides:
Hawaii, Indiana, Maine, Mississippi, Missouri, Nevada

(a) Use of criminal history record information disseminated to noncriminal justice agencies shall be restricted to the purpose for which it was given.

(b) No criminal justice agency shall disseminate criminal history record information to any person or agency . . . unless said person or agency enters into a user agreement with the Bureau, which agreement shall:

1. Specifically authorize access to the data or information;
2. Limit the use of the data or information to purpose for which it was given;
3. Ensure the security and confidentiality of the data or information consistent with this chapter . . . .


109. Hawaii’s statute provides:

Dissemination of nonconviction data shall be limited, whether directly or through any intermediary, only to:

1. Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment . . . .

2. Criminal history record information disseminated to noncriminal justice agencies shall be used only for the purposes for which it was given.

3. No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.


110. Indiana’s statute states:

A noncriminal justice organization or individual that receives a limited criminal history may not use it for purposes: (1) other than those stated in the request; or (2) that deny the subject any civil right to which the subject is entitled.

Ind. Code Ann. § 10-13-3-29 (West 2004).

111. Maine’s statute provides:

Criminal history record information disseminated to a noncriminal justice agency . . . shall be used solely for the purpose of which it was disseminated and shall not be disseminated further.


112. Mississippi’s statute states:

2. Information disseminated for noncriminal justice purposes as specified in this section shall be used only for the purpose for which it was made available and may not be re-disseminated . . . .

8. Release of the above-described information for noncriminal justice purposes shall be made only by the center, under the limitations of this section, and such compiled records will not be released or disclosed for noncriminal justice purposes by other agencies in the state.


113. Missouri’s statute provides:

[T]he sheriff of any county, the sheriff of the city of St. Louis, and the judges of the circuit courts of this state may make available, for review, information obtained from the central repository to private entities responsible for probation supervision . . . . When the term of probation is completed or when the material is no longer needed for purposes related to the probation, it shall be returned to the court or destroyed. The private entities shall not use or make this information available to any other person for any other purpose.
Tennessee,\textsuperscript{115} and Washington\textsuperscript{116}, the devil is in the details. In the

MO. ANN. STAT. §§ 43.504, 43.540 (West Supp. 2010). Another Missouri statute provides:

Any information received by an authorized state agency or a qualified entity pursuant to the provisions of this section shall be used solely for internal purposes in determining the suitability of a provider. The dissemination of criminal history information from the Federal Bureau of Investigation beyond the authorized state agency or related governmental entity is prohibited. All criminal record check information shall be confidential and any person who discloses the information beyond the scope allowed is guilty of a class A misdemeanor.

MO. ANN. STAT. § 43.540(5) (West Supp. 2010).

114. Nevada’s statute provides:

A record of criminal history or any records of criminal history of the United States or another state obtained pursuant to this chapter must be used solely for the purpose for which the record was requested. No person who receives information relating to records of criminal history pursuant to this chapter . . . may disseminate the information further without express authority of law or in accordance with a court order. This section does not prohibit the dissemination of material by an employee of the electronic or printed media in a professional capacity for communication to the public.


115. Tennessee’s statute states:

(a) The Tennessee bureau of investigation shall process requests for criminal background checks from any authorized persons, organizations or entities permitted by law to seek criminal history background checks on certain persons, pursuant to a format and under procedures as it may require . . . .

(c)(1) Agencies or organizations that have an agreement to do so with the Tennessee bureau of investigation and that have any responsibility or authority under law for conducting criminal history background reviews of persons may also access directly the computer files of the T.C.I.C. using only names or other identifying data elements to obtain available Tennessee criminal history background information for purpose of background reviews.

TENN. CODE ANN. § 38-6-109(a), (c)(1) (2010).

116. Washington’s statute provides:

(3) Criminal history record information which includes nonconviction data may be disseminated by a criminal justice agency to another criminal justice agency for any purpose associated with the administration of criminal justice, or in connection with the employment of the subject of the record by a criminal justice or juvenile justice agency

(4) [Or] to implement a statute, ordinance, executive order, or a court rule, decision, or order which expressly refers to records of arrest, charges, or allegations of criminal conduct or other nonconviction data and authorizes or directs that it be available or accessible for a specific purpose.

(5) Criminal history record information . . . may be disseminated to individuals and agencies pursuant to a contract with a criminal justice agency to provide services related to the administration of criminal
brick-and-mortar world where background checks were performed by a local service it was easy for government agencies to impose sanctions in response to improper use; in a virtual, Internet-connected world this is much more difficult.

It is even less effective to require government workers to mandate that a private employer sanction or terminate an employee who violates the rules. It is more burdensome to audit private entities, especially when they are located out-of-state (or country). Even in an era when providing government data meant sliding paper copies across a countertop, because of these burdens it was only marginally effective to mandate that government workers limit dissemination of criminal justice system users who agreed to use it properly, or who agreed not to secondarily disseminate it (for examples of restrictions on re-dissemination, see statutes in Arizona, Arkansas, Idaho, Maine, Mississippi, Missouri, Nevada, Pennsylvania, Wyoming, and

justice . . . .
(6) [Or] to individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency . . . .


118. ARK. CODE ANN. § 12-12-1009 (b) (2009) (“Dissemination of conviction information for noncriminal justice purposes. . . . (b) Conviction information disseminated for noncriminal justice purposes under this subchapter shall be used only for the purposes for which it was made available and may not be redisseminated.”).

119. Idaho’s statute states:
Release of criminal history record information. . . . (6) A person or private agency, or public agency, other than the department, shall not disseminate criminal history record information obtained from the department to a person or agency that is not a criminal justice agency or a court without a signed release of the subject of record or unless otherwise provided by law.


120. ME. REV. STAT. ANN. tit. 16, § 617 (2006).


122. MO. ANN. STAT. § 43.504 (West 2001).


124. Pennsylvania’s statute states:
Secondary dissemination prohibited—A criminal justice agency which possesses information protected by this section, but which is not the source of the information, shall not disseminate or disclose the information to another criminal justice agency but shall refer the requesting agency to the agency which was the source of the information.

18 PA. STAT. ANN. § 9106 (d) (West 2000).

125. Wyoming’s statute, titled Access to and Dissemination of Information,
The government agency tasked to ensure proper use cannot perpetually babysit the data in the hands of the private company, so it must engineer an audit process (especially burdensome when the business being audited is located in another jurisdiction) or wait for those damaged by a violation to complain of misuse. Once such misuse comes to light, the responsible government agency must either press the local prosecutor into service where the violation is criminalized, or rely on the state’s attorney general to pursue a civil remedy. Faced with plenty of in-state crime-against-person felony charges to pursue, prosecutors likely do not consider data use violations a high priority. Relying on the civil bar to pursue

---

Connecticut.

Further provisions for disclosure of nonconviction information. Nonconviction information other than erased information may be disclosed only to: (1) Criminal justice agencies in this and other states and the federal government; (2) agencies and persons which require such information to implement a statute or executive order that expressly refers to criminal conduct; (3) agencies or persons authorized by a court order, statute or decisional law to receive criminal history record information. Whenever a person or agency receiving a request for nonconviction information is in doubt about the authority of the requesting agency to receive such information, the request shall be referred to the state police bureau of investigation.

**CONN. GEN. STAT. ANN. § 54-142n** (West 2009).

**CONN. GEN. STAT. ANN. § 54-142o** (a). “Dissemination of nonconviction information to noncriminal justice agencies. (a) Nonconviction information disseminated to noncriminal justice agencies shall be used by such agencies only for the purpose for which it was given and shall not be redisseminated.”

**127.** See, e.g., **MO. ANN. STAT. § 43.532** (2) (West Supp. 2010). Missouri’s statute states:

Use of records, limitations—authority of central records repository to retain information—unlawful obtaining of information, penalty. . . . 2. The central records repository shall have authority to engage in the practice of collecting, assembling, or disseminating criminal history record information for the purpose of retaining manually or electronically stored criminal history information. Any person obtaining criminal history record information from the central repository under false pretense, or who advertises or engages in the practice of collecting, assembling, and disseminating as a business enterprise, other than for the purpose of furnishing criminal history information to the authorized requester for its intended purpose, is guilty of a class A misdemeanor.
damages for those hurt by violation of data use violations is problematic as well. The population that tends to be disadvantaged by such violations is the same population that interacts frequently with the criminal justice system: that is, those more likely to be transient and indigent and not ideal clients to be represented by lawyers pursuing prolonged civil litigation.

In the context of the MGDPA’s policy of open government data, it is difficult to imagine a “data babysitting” requirement that could help the young soldier avoid having the mistaken record come back from the world of commercial data harvesters to haunt him.

3. Discourage Use for Casual or Frivolous Purposes

Rather than implement use limitations that would require a “data babysitter” for effective enforcement, some states have instead tried to increase the cost of data harvesting by addressing the market created by curiosity-seekers and casual snoops. Colorado\(^{128}\) and Rhode Island\(^{129}\) make data available but prohibit recipients from selling it. Arizona requires payment of a fee.\(^\text{130}\)

In contrast, Minnesota came up with a much more conservative approach. Policymakers balanced the desire for open government data with the benefits of rehabilitating criminal offenders and produced the Criminal Offender Rehabilitation Act

\(^{128}\)Colorado’s statute states:
Access to records—denial by custodian—use of records to obtain information for solicitation. Records of official actions and criminal justice records and the names, addresses, telephone numbers, and other information in such records shall not be used by any person for the purpose of soliciting business for pecuniary gain. The official custodian shall deny any person access to records of official actions and criminal justice records unless such person signs a statement which affirms that such records shall not be used for the direct solicitation of business for pecuniary gain.

\(^{129}\)Rhode Island’s statute states:
Commercial use of public records—No person or business entity shall use information obtained from public records pursuant to this chapter to solicit for commercial purposes or to obtain a commercial advantage over the party furnishing that information to the public body. Anyone who knowingly and willfully violates the provision of this section shall, in addition to any civil liability, be punished by a fine of not more than five hundred dollars ($500) and/or imprisonment for no longer than one year.

(CORA), which prohibits use of arrest data not leading to conviction but only in circumstances where government employers are considering employment applications. Private employers and landlords remain free to use unproven accusations to make decisions about applicants.

Many times in recent years, legislative subcommittees in Minnesota have considered the idea of limiting availability or use of arrest data not leading to conviction. Landlord groups, chambers of commerce, and data harvesters are well-represented among the ranks of lobbyists who work in Minnesota’s State Capitol, and their arguments supporting continued ability to see and to use such unproven accusation data are based upon the possibility that an arrest really can suggest guilt. Presumption of innocence is a fine abstraction for the courtroom, they argue, but the Constitution does not demand it for the rest of us as we make decisions in our daily lives and business dealings. A school bus company ought to be able to reject an applicant for a driver’s job because she has been charged with, but not convicted of, reckless driving and DUI; a landlord screening applications for an apartment building ought to be able to say no to a tenant with multiple charges of, but no convictions for, sexual assault. The burden of proof necessary to support a criminal conviction—proof beyond a reasonable doubt—is the highest the law provides. This is as it should be, as it regulates the government’s ability to deprive an individual of freedom. Nothing in constitutional law imposes any similarly high standard upon decisions made outside of criminal courtrooms.

131. Minnesota’s statute states:
Availability of records. The following criminal records shall not be used, distributed, or disseminated by the state of Minnesota, its agents or political subdivisions in connection with any application for public employment nor in connection with an application for a license: (1) Records of arrest not followed by a valid conviction.

It is easy to imagine what goes through the head of a legislator who is asked to sponsor a bill that would make inaccessible all arrest records not leading to conviction: when the fully-loaded school bus (driven by the driver with unavailable arrest data) plunges into the ravine, what is that going to be like?

To date, these arguments have convinced lawmakers to keep all arrest records not leading to conviction accessible to the public, except for the fairly minor exception found within CORA.

V. MINNESOTA’S PROGRESS TOWARD APPLYING FAIR INFORMATION PRINCIPLES TO COMMERCIAL DATA MINING OF CRIMINAL JUSTICE SYSTEM RECORDS

When Minnesota’s data policy pioneers developed the nation’s premier model of government records transparency, they anticipated that data-handling technologies would evolve. But they could not have imagined that three and a half decades later the smallest government records were to be made instantaneously and irretrievably available worldwide. Minnesota has a problem: its government’s transparency fuels unregulated commercial data mining activities that hurt people.

Recognizing that the relationship between government and data harvesters can result in this damage, all three branches of government have made strong policy statements. The Minnesota Supreme Court makes records of unproven accusations available only to people who come to the courthouse to search for them; they are not posted on the court’s public web site. The Minnesota Legislature passed and the Governor signed into law a requirement that “business screening services” enhance the reliability of their data by updating harvested records within a month before they are disseminated. This law makes it more likely that a record of an accusation will be disseminated along with the record of its dismissal or an acquittal, a significant benefit for the tens of thousands of individuals charged with but never convicted of low-level misdemeanor crimes.

133. The Rules Of Public Access To Records Of The Judicial Branch, supra note 44.
134. See Minn. Stat. § 332.70 (Supp. 2010).
135. See Sykora, supra note 10 (showing court data that sixty percent of such charges result in acquittal or dismissal, and another study showing that 21.9% of such charges resulted in conviction).
At the Minnesota Legislature, discussion began in 2009 about a bill with language intended to enhance transparency by requiring users of online background checks to notify data subjects when such a check will be made, and informing data subjects of the steps necessary to obtain a free copy of the results.\textsuperscript{136} As this approach is aimed at the \textit{consumers} of data located in Minnesota rather than foreign-located, web-based services, enforcement is more likely to be effective. Though the transparency language was not passed into law during the most recent legislative session, it is likely to be re-introduced in 2011.

Enhancing data reliability may be possible, though costly, by requiring peace officers to utilize portable fingerprint readers (generically described as “two-finger rapid ID” devices) in circumstances where an individual does not produce a driver’s license. Such a fingerprint check may have prevented damage to the reputation of the young soldier discussed in this article.

Finally, we must recognize that commercial data mining of criminal justice records has a harsh effect upon those least likely to have the resources to protect themselves. Minnesota can take a strong step to ameliorate that harshness by expanding CORA\textsuperscript{137} to the private sector. CORA currently prohibits only government employers from making hiring decisions based on arrests not followed by conviction, or by expunged convictions, or by misdemeanor convictions where a jail sentence cannot be imposed.\textsuperscript{138} In some areas, a criminal conviction may disqualify an applicant only if the crime relates directly to the type of employment sought and the applicant is unable to show that he has been rehabilitated. The law has provisions requiring notice to the applicant about the data underlying reasons for rejection and the steps an applicant may take to exercise rights under CORA.


\textsuperscript{137} MINN. STAT. § 364.04 (2004 & Supp. 2010).

\textsuperscript{138} \textit{Id.}
CORNA finds a sensible balance between open records on one hand and the rights of data subjects on the other. The law successfully has regulated tens of thousands of government hiring processes since it went into effect at just about the same time Minnesota put the MGDPA in place. Applying CORA to the private sector would restore some of the balance lost when “open records” inadvertently came to mean instant, global, and perpetual data availability.

VI. CONCLUSION

I laugh when I recall a cartoon that dates back to the era when we all were getting used to the strange anonymity of interaction using the Internet. A sincere looking beagle sits with his paws on a computer keyboard, commenting to another canine: “On the Internet, nobody knows you’re a dog.” Fifteen years later, the joke has evolved along with our fears and anxieties. Today, at least when considering criminal justice data in an unregulated background check, everyone assumes you’re a dog.