2013

The Hidden Costs of Terrorist Watch Lists

Anya Bernstein

BUFFALO LAW REVIEW

VOLUME 61 MAY 2013 NUMBER 3

The Hidden Costs of Terrorist Watch Lists

ANYA BERNSTEIN†

INTRODUCTION

The No Fly List, which is used to block suspected terrorists from flying, has been in use for years. But the government still appears "stymied" by the "relatively straightforward question" of what people who "believe they have been wrongly included on" that list should do.[1] In recent months, courts have haltingly started to provide their own answer, giving some individuals standing to sue to remove their names or receive additional process.[2] This step is particularly important as the No Fly List continues

† Bigelow Fellow and Lecturer in Law, The University of Chicago Law School. J.D., Yale Law School; Ph.D., Anthropology, The University of Chicago. Thanks to Daniel Abebe, Ian Ayres, Alexander Boni-Saenz, Anthony Casey, Anjali Dalal, Nicholas Day, Bernard Harcourt, Aziz Huq, Jerry Mashaw, Jonathan Masur, Nicholas Parrillo, Victoria Schwartz, Lior Strahilevitz, Laura Weinrib, Michael Wishnie, and James Wooten for helpful commentary.

1. Latif v. Holder, 686 F.3d 1122, 1130 (9th Cir. 2012) (characterizing the government's response to questions at oral argument).

2. *Id.* (holding that United States citizens and legal, permanent residents who suspect they are listed on the No Fly List have standing to sue for an injunction ordering the government to remove their names or to provide additional process); Ibrahim v. Dep't of Homeland Sec., 669 F.3d 983, 999 (9th Cir. 2012) (noting the same for an alien with substantial voluntary connections to the United States). Because the criteria for adding someone to the No Fly List are secret, it will no doubt be a challenge for both courts and government to determine how to implement any additional process due to those listed on it. Peter Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804, 837-54 (2007) (outlining a due process regime that takes into account both the rights of individuals and the needs of the government).

its breathtaking growth.[3] It is unclear, however, how a court will evaluate that additional process when the listing criteria are both secret and untested. This doctrinal development poses a challenge not only to the No Fly List, but also to the complex watch list infrastructure on which it is built.

The No Fly List draws on a consolidated terrorist watch list that compiles numerous other lists maintained by a number of federal agencies.[4] Agencies compiling their lists receive information not only from their own agents but from state governments, foreign nations, and private individuals.[5] The No Fly List is well known because it has visible effects like impinging on rights to travel. Indeed, it is precisely such effects that have led courts to recognize standing to challenge them.[6] But the No Fly List's flaws are inherited from the lists it uses. They, in turn, remain largely unregulated, unappealable, and obscured from public attention.

Commentators have argued that such watch lists raise problems for privacy and due process rights.[7] This Article

---

3. *See* Associated Press, *U.S. No-Fly List Doubles in One Year*, U.S.A. TODAY (Feb. 2, 2012, 11:02 AM), http://usatoday30.usatoday.com/news/washington/story/2012-02-02/no-fly-list/52926968/1 (reporting that the No Fly List increased from "about 10,000 known or suspected terrorists one year ago to about 21,000" in February 2012).

4. Shane, *supra* note 2, at 807-08.

5. The precise number of watch lists, as well as of names on watch lists, is difficult to ascertain because publicly available information is limited. *See id.* at 813-14 (tabulating watch lists maintained by federal agencies). For instance, while internal FBI documents reveal the construction of a new Known and Suspected Terrorist list in 2009, there is no public information about this list. *CJIS Advisory Policy Board Working Group Meetings Spring 2009, Staff Paper* 4-5 (document produced in FOIA litigation) (Bates No. NCIC-VGTOF-8334-35) (on file with author). The FBI has not published a System of Records Notice about the new list in the Federal Register, as required by statute. *See* 5 U.S.C. § 552a(e)(4) (2006) (providing no relevant System of Records Notice).

6. *See, e.g.*, *Ibrahim*, 669 F.3d at 987, 993-94 (determining that plaintiff had standing because being placed on the No Fly List restricted her ability to travel even when the destination was not the United States and restricted her ability to associate with others by attending academic conferences).

7. *See* Michael German & Jay Stanley, *What's Wrong with Fusion Centers?*, AM. CIVIL LIBERTIES UNION, 3 (2007), http://www.aclu.org/technology-and-liberty/whats-wrong-fusion-centers-executive-summary.

broadens the frame, moving beyond individual rights to the broader effects that watch lists have on the agents and agencies who run them, the government that commissions them, and the society that houses them. It also explains why agencies currently lack the incentives to address these problems themselves. Because current law fails to rein watch lists in, they require external constraint. Focusing on watch lists' peculiar epistemological and social structure, this Article identifies the key aspects of watch list creation that require regulation. And it draws on developments in regulatory theory to ground its proposals for reform.

This Article starts with the question of why watch lists require more constraint to begin with. Legal constraints, after all, usually exist to make people do things they would not otherwise do. And at first glance, there seems to be every reason to think that government agencies want to make their watch lists work. If that is the case, we can assume that agencies will try their hardest to create the best and most useful watch lists possible. We would not need to tell them how, or to force them to take some particular route to getting there.

As I contend in Part I, however, the incentive structures surrounding terrorist watch lists push agents and agencies to exaggerate dangers, putting names on watch lists that do not belong there. These false positives might be more acceptable if they made watch lists more comprehensive, reducing the likelihood that the watch list would miss someone who ought to be on there—a false negative. But, as Part I also shows, watch lists' perverse incentives lead agents and agencies to misconstrue the relationship between false positives and false negatives. These perverse effects endanger the very national security that watch lists are meant to safeguard by discouraging the kind of self-correction that would make watch lists more effective.

Part II explains the structure of contemporary terrorist watch lists, showing how information and knowledge are produced in the watch list context. Contemporary watch lists use the techniques of "big data" to collect information and distribute the work of evaluation and prediction over many participants.[8] However, they largely eschew the self-

8. "Big data" broadly refers to the use of unprecedented quantities of data for natural- and social-scientific analysis. The hope of big data users is to harness large data sets to make interpretations and predictions independently

assessment techniques that make the use of big data reliably useful. Their distributed knowledge production can help watch lists smooth over the peculiarities of individual agents. But it can also exacerbate judgment problems by stacking peculiarity upon peculiarity and giving the result a veneer of objective truth. Explaining how judgment is incorporated in watch lists elucidates the errors they are prone to and helps clarify why a conflicted incentive structure leads to a high false positive rate.

A high rate of false positives might still be acceptable if there were no cost associated with them. And because of their objective veneer, watch lists can seem like a costless, neutral backdrop of impartial information about the world. It seems as though they have no effects on the world themselves. Part III argues that this neutral view is wrong. As scholars concerned with individual rights have recognized, unregulated, error-prone watch lists affect the people listed on them in powerful ways. But watch lists also affect the agents and agencies that maintain them, lowering their efficacy and acumen by failing to provide reality checks for their judgments. Further, watch lists skew public policy by making terrorism appear to be a more imminent and severe threat than it is, which leads resources to be diverted from other programs into terrorism-related ones.[9] And to the broader public, watch lists present a world populated by terrorist threats that can often be recognized with blunt categories like ethnicity and religion. That

of small variations across populations. The fears of their critics are that big data usage techniques focus so much on the control of data itself that they neglect testing the accuracy, or the normative implications, of their results. *See, e.g.*, *Data, Data Everywhere*, THE ECONOMIST, Feb. 27, 2010, at 1-2 (reporting that scientists and businesses have access to vastly more data than ever before and explaining that this so-called big data poses unprecedented opportunities for uncovering social trends and scientific truths, but also poses new challenges in data management and interpretation); Alan Feuer, *The Mayor's Geek Squad*, N.Y. TIMES, Mar. 24, 2013, at MB1; Steve Lohr, *Origins of 'Big Data': An Etymological Detective Story*, N.Y. TIMES BITS BLOG (Feb. 1, 2013, 9:10 AM), http://bits.blogs.nytimes.com/2013/02/01/the-origins-of-big-data-an-etymological-detective-story/ (discussing difficulty of tracing the origin of the term "big data" and giving the most likely sources); Press Release, Office of Science and Technology Policy, Executive Office of the President, Obama Administration Unveils "Big Data" Initiative: Announces $200 Million in New R&D Investments (Mar. 29, 2012), http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf.

9. GERMAN & STANLEY, *supra* note 7, at 22-23.

affects how people act in their society and what they see as its most urgent problems. Watch lists, in other words, are far from costless. They go beyond affecting individual rights to affect government functioning and social structure.

Yet, as Part IV claims, the legal strictures that currently regulate database use miss the point. They focus on informational accuracy, not predictive efficacy. I suggest that this lacuna rests on an outdated understanding of contemporary databases as mere repositories for independently existing information, not the sites of judgment production and prediction they actually are.

Traditionally, government judgment has been subject to legal constraint that can be reviewed in court. The watch list context, as I show, complicates this approach by introducing secret algorithms of prediction that result in little that is cognizable in court. This limitation, I contend, should not dissuade us from analyzing and constraining watch lists. The absence of judicial review cannot obviate scrutiny and constraint of government action in a democratic society. Rather, as recent scholarship has suggested, we must look to institutional design and internal self-regulation to solve those problems that cannot reach the courts.[10]

Part V proposes regulating watch lists by focusing on the increased efficacy that comes with increased constraint. My suggestions build on a growing call for government to assess, and not only project, the effects of its actions. And they stake a claim for Bayesian updating at the center of administrative self-regulation—the kind of regulation that increasingly looks to be the main way of controlling the administrative state.[11]

Finally, the Conclusion examines the limitations of my proposals and explains why any solution to the watch list problem will always be partial. It further discusses how similar concerns, and a similar approach, will be appropriate to other government databases used to make predictions about future human conduct, when their incentive structures are similarly conflicted.

---

10. *See* Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2319-24 (2006).

11. *See, e.g.*, *id.* at 2316.

I. WHY ARE TERRORIST WATCH LISTS NOT SELF-REGULATING?

To the extent that terrorist watch lists play a role in national security, we would expect the agencies that manage them to create strict procedures to ensure their efficacy. Given how central national security is to contemporary government, the incentives for efficacy should be so strong that such lists would not require additional regulation. In actuality, however, agencies have not fulfilled these expectations. Below, I explain how conflicts in the agencies' incentive structure cause this failure. I also explain how mistaken assumptions about the relationship between false positives and false negatives in the watch list context make the failure to implement internal regulation seem less important than it is.

A. *Incentive Failures*

Reports indicate that people are commonly listed in terrorist watch lists based on suspicions ranging from the constitutionally impermissible to the absurd. For example, in 2012, the Department of Homeland Security (DHS) detained and refused entry to two British nationals en route to Los Angeles because the agency concluded that the couple's Twitter messages suggested they were planning to engage in terrorist activity.[12] DHS did not credit the tourists' claim that they were joking when they announced on Twitter that they planned to "dig up" Marilyn Monroe, nor that a tweet about "destroy[ing] America" simply used British slang for "party."[13]

In another scenario, reminiscent of the Federal Bureau of Investigation's (FBI's) notorious CoIntelPro operations,[14]

---

12. *See* Richard Hartley-Parkinson, *'I'm Going to Destroy America and Dig Up Marilyn Monroe': British Pair Arrested in U.S. on Terror Charges over Twitter Jokes*, MAIL ONLINE (Jan. 31, 2012, 8:08 AM) http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html.

13. *Id.*

14. The FBI describes its CoIntelPro operations in this way:

> The FBI began COINTELPRO—short for Counterintelligence Program—in 1956 to disrupt the activities of the Communist Party of the United States. In the 1960s, it was expanded to include a number of other domestic groups, such as the Ku Klux Klan, the Socialist Workers

the Denver police department "built a computer database full of personal details about people" engaging in constitutionally protected activity, such as being "active in political groups" like "a Quaker peace-advocacy group . . . and . . . the pro-gun lobby."[15] Because terrorist watch lists often gather records from local law enforcement agencies, entries in such databases can lead extensive lives outside the local law enforcement agency itself. Although the Denver files were expunged after a Freedom of Information Act suit made them public, "when a man listed in the Denver files as a gun-rights group member got into a fender bender, a police officer checking [an FBI terrorist watch list] found him described as 'a member of a terrorist organization' [and] reported the stop to the FBI as a 'terrorist contact.'"[16] The man's record, in other words, had made its way into the federal terrorist watch list; but its subsequent expungement had not.

Yet more troublingly, agencies that manage watch lists have been reluctant to create ways to improve—or even evaluate—their efficacy. The Transportation Security Administration, for instance, "operated its data-based passenger screening programs for more than two years with no system in place to report or correct errors," despite its famously high error rate.[17] And in recent years, federal agencies have increasingly exempted law enforcement and national security databases from Privacy Act provisions

---

Party, and the Black Panther Party. All COINTELPRO operations were ended in 1971. Although limited in scope (about two-tenths of one percent of the FBI's workload over a 15-year period), COINTELPRO was later rightfully criticized by Congress and the American people for abridging first amendment rights and for other reasons.

See FBI Records: The Vault, FBI: THE FEDERAL BUREAU OF INVESTIGATION, http://vault.fbi.gov/cointel-pro (last visited Apr. 6, 2013).

15. Ann Davis, *Use of Data Collection Systems Is Up Sharply Following 9/11*, WALL ST. J., May 22, 2003, at B1.

16. *Id.* As this report indicates, records entered into one law enforcement database can take on a life of their own as they are distributed to others, often with no provisions for updating the secondary files when the original one changes. *Id.*

17. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 475 (2008).

requiring agencies to ensure their records are accurate, relevant, timely, and complete.[18]

For instance, agencies have exempted a number of databases collected by the Terrorist Screening Database (TSDB) from these statutory provisions. And in 2003, the FBI exempted the entire National Crime Information Center (NCIC) database,[19] which holds a wealth of information, including the names of people the FBI or the Terrorist Screening Center (TSC) suspect of belonging to terrorist groups or planning to engage in terrorist acts.[20]

---

18. The Privacy Act allows certain agencies to exempt some records from some of its provisions under certain circumstances. *See* 5 U.S.C. § 552a(e)(5) (2006).

19. *See* Privacy Act of 1974; Implementation, 68 Fed. Reg. 4974 (proposed Jan. 31, 2003) (to be codified at 28 C.F.R. § 16.96); Privacy Act of 1974; Implementation, 68 Fed. Reg. 14,140 (Mar. 24, 2003) (codified at 28 C.F.R. § 16.96); *see also* 28 U.S.C. § 534(a)(1) (2006) (providing that "[t]he Attorney General shall . . . acquire, collect, classify, and preserve identification, criminal identification, crime, and other records"); Interstate Identification Index (III), SEARCH http://www.search.org/programs/policy/iii/ (last visited Mar. 5, 2013) (stating that the Interstate Identification Index holds records of convictions as well of arrests for felonies and serious misdemeanors). For a description of the NCIC, see *National Crime Information Center*, FBI: THE FEDERAL BUREAU OF INVESTIGATION, http://www.fbi.gov/hq/cjisd/ncic.htm (last visited Mar. 5, 2013).

20. *See* Privacy Act of 1974; Modified System of Records, 60 Fed. Reg. 19,774, 19,774-75 (Apr. 20, 1995) (issuing a System of Records Notice for the Violent Gang and Terrorist Organization File (VGTOF)); *see generally Passport Information Sharing with Department of State: Hearing Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 109th Cong. 2 (2005) (statement of Donna A. Bucella, Dir., Terrorist Screening Ctr.) (describing the Terrorist Screening Center's (TSC's) consolidation of names of known and suspected terrorists into the Terrorist Screening Database (TSDB)); WILLIAM J. KROUSE, CONG. RESEARCH SERV., RL 32366, TERRORIST IDENTIFICATION, SCREENING, AND TRACKING UNDER HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 6, at 31-32 (citing unpaginated front matter) (2004) (noting that the NCIC is used to disseminate records from the TSC's TSDB).

The most plausible reading of the Privacy Act suggests that the VGTOF is actually not subject to exemption. The exemption notice states that the "exemptions apply only to the extent that information in the system is subject to exemption pursuant to" sections (j)(2) and (k)(3) of 5 U.S.C. § 552a. 28 C.F.R. § 16.96(g)(1) (2012). Section (j)(2) allows a law enforcement agency to exempt a system of records containing 1) "information compiled for the purpose of identifying individual criminal offenders and alleged offenders"; 2) "information compiled for the purpose of a criminal investigation"; or 3) "reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision." 5

Any law enforcement agent in the country can access the NCIC. Officers routinely use the NCIC during common interactions with the public, such as traffic stops, to check whether an individual is listed in its terrorist watch list, among other things.

The notice exempting the NCIC asserted that "ensur[ing] compliance with" the Privacy Act's requirements that information be accurate, relevant, timely, and complete was "administratively impossible" "because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies."[21] It also noted that, "[w]ith the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light."[22]

As the exemption notice suggests, terrorist watch lists create a particularly shaky form of prediction for a number

---

U.S.C. § 552a(j)(2) (2006). Under section (k)(3), an agency may exempt records maintained for the President's protective services. 5 U.S.C. § 552a(k)(3) (2006*; see also* 18 U.S.C. § 3056(a)(1) (describing the authorization of the United States Secret Service to protect the President). VGTOF records, however, do not identify alleged criminal offenders, are compiled separately from criminal investigations and enforcement operations, and do not concern the protective services. The proffered exemptions thus do not apply to VGTOF files. The exemption would be difficult to challenge, however, for standing reasons. *See* discussion *infra* Part IV.B.

21. 28 C.F.R. 16.96(b)(6) (2012).

22. Privacy Act of 1974; Implementation, 68 Fed. Reg. at 14,140. The notice of final rulemaking does not address any public comments and does not mention whether any comments were received in response to the notice of proposed rulemaking. The contention that seemingly unimportant discrete pieces of information must be collected and protected from exposure because they may end up fitting together in some important but unpredictable way is sometimes called the "mosaic theory." The mosaic theory posits that, because seemingly unimportant discrete pieces of information may end up fitting together in an important but unpredictable way, they should be assiduously collected and protected from disclosure. David E. Pozen, Note*, The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 633 (2005). The theory has been criticized for encouraging an over inclusion of information, overemphasis on secrecy, and general inefficacy. *Id.* at 632-33. Moreover, while the mosaic theory holds that any piece of information may be useful someday, it operates in a world of limited resources, where someone must determine which pieces of information are worth collecting, keeping, and analyzing. *See id.* at 630. Mosaic theory claims thus obscure the decisions that unavoidably go into information collection and data processing.

of reasons. Human conduct is especially difficult to predict in areas with little historical data to draw on.[23] Terrorists tend to organize themselves in ways that are less structured and regular than some other forms of social organization.[24] And it is hard to approach emotionally salient topics with the kind of dispassionate attitude that facilitates rational projections.[25]

These difficulties should lead agencies to impose more, not less, oversight on terrorist watch lists. And because the Privacy Act does not define accuracy, relevance, timeliness, and completeness, the agency could have issued regulations interpreting them in the context of the NCIC. Instead, it exempted the database from Privacy Act requirements by claiming that the database's weaknesses are unknowable to the very agency that maintains it, and that this opaqueness itself excuses the agency from setting standards for it. That explanation itself, of course, raises the question of why

---

23. Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, 584 CATO INST. POL'Y ANALYSIS 1, 7-8 (2006). Jonas and Harper explain that predictions made through data mining work best when based on a wealth of historical information about how people behave under various circumstances, but become much less reliable when less historical data is available. They emphasize that very little historical data is available on terrorists and terrorism. Moreover, focusing merely on unusual behavior cannot effectively predict terrorist conduct: "Treating 'anomalous' behavior as suspicious may appear scientific, but, without patterns to look for, the design of a search algorithm based on anomaly is no more likely to turn up terrorists than twisting the end of a kaleidoscope is likely to draw an image of the Mona Lisa." *Id.* at 8.

24. Karin Knorr Cetina, *Complex Global Microstructures: The New Terrorist Societies*, 22 THEORY, CULTURE & SOC'Y 213, 214 (2005) (suggesting that contemporary terrorism manages to extend its reach by "avoid[ing] complex institutional structures" that allow a greater measure of prediction; rather, it exhibits the "asymmetries, unpredictabilities and playfulness of complex (and dispersed) interaction patterns"); *see also* TODD MASSE, SIOBHAN O'NEIL, AND JOHN ROLLINS, CONG. RESEARCH SERV., RL 33858, THE DEPARTMENT OF HOMELAND SECURITY'S RISK ASSESSMENT METHODOLOGY: EVOLUTION, ISSUES, AND OPTIONS FOR CONGRESS: SUMMARY (2007), *available at* http://fpc.state.gov/documents/organization/80208.pdf (noting that risk assessment in the national security field is particularly difficult because of "the dynamic nature of terrorism" and the absence of specific historical evidence).

25. Dan M. Kahan et al., *'They Saw a Protest': Cognitive Illiberalism and the Speech-Conduct Distinction*, 64 STAN. L. REV. 851, 900 (2012) (arguing that cultural and emotional commitments lead people to radically different interpretations of the same events).

every routine interaction between law enforcement agents and private individuals should include a check of a watch list whose quality and utility is simply not knowable.

This reluctance to increase efficacy by assessing it seems particularly out of place in the national security context, where stakes are high. But growing evidence indicates that this attitude is not unusual in the national security arena. A recent National Research Council study found that, while DHS has developed adequate risk analysis protocols for addressing natural disasters, it has no risk analysis framework for terrorism threats.[26] Relatedly, researchers have found that DHS rebuffs requests to conduct risk or cost-benefit analyses for national security-related regulations.[27] DHS asserts that the dynamic and evolving nature of national security risk makes such analysis impossible.[28] Thus, the department promulgates regulations while asserting that it can have no opinion about their utility.[29]

This trend might not be so worrisome if terrorist watch lists were subject to incentives that would assure that agencies would strive for the highest level of efficacy even if they did not publicize their processes for doing so. Unfortunately, that too is not the case. Terrorist watch lists may appear to serve a single purpose: to help the government prevent terrorist attacks by keeping track of suspected terrorists. But like other predictive database uses, they actually serve multiple, competing purposes, which subject government agents to conflicting pressures.

Specific goals like preventing terrorism are couched in larger obligations like serving the public good and treating

---

26. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S APPROACH TO RISK ANALYSIS 2 (2010).

27. JOHN MUELLER & MARK G. STEWART, TERROR, SECURITY, AND MONEY: BALANCING THE RISKS, BENEFITS, AND COSTS OF HOMELAND SECURITY 5 (2011).

28. *Id.*

29. This comports with scholarship finding that political salience affects the substance of proposed regulations. *See* Stuart Shapiro & John F. Morrall III, *The Triumph of Regulatory Politics: Benefit–Cost Analysis and Political Salience*, 6 REG. & GOVERNANCE 189, 190 (2012) (finding that politically salient proposed rules tend to have smaller projected benefits than lower-salience rules).

people fairly.[30] Those larger obligations, in turn, have many interpretations. In one familiar juxtaposition, some define the public good in terms of community security while others focus on individual privacy.[31] Still others have other definitions. Some may view restraining the government's intervention in society as a public good, while others view the government's role as ensuring fair treatment and safety for all. Because what best serves the public good and what constitutes fairness are subjects of debate in democratic societies, these larger obligations are never finally defined or uniform among participants.

These varied goals, moreover, coexist with other motivations. Agents and agencies have performative incentives to appear active and efficacious. And they have rent-seeking incentives to ensure continued resources and attention to their operations. One way of showing that an agency that maintains a watch list is active and efficacious is to put more names on the list. Agencies that keep watch lists may face image problems when they list people who are unlikely to fulfill their predictions.[32] But they may also benefit from listing more people at the expense of accuracy. More entries can make the agency look more active in its pursuit of the public good, even when they produce no actual public benefits down the line.

---

30. Program Manager, Info. Sharing Env't, *Information Sharing Environment Annual Report to the Congress, National Security Through Responsible Information Sharing*, at iv (June 30, 2012), http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2012.pdf (noting that the agency had recently strengthened privacy and civil rights safeguards on terrorism related information-sharing).

31. *See, e.g.*, John T. Soma et al., *Balance of Privacy vs. Security: A Historical Perspective of the USA PATRIOT Act*, 31 RUTGERS COMPUTER & TECH. L.J. 285, 287 (2005) (positing that public sentiment tends to swing toward preferring national security following a crisis but returns to "equilibrium . . . as the initial threat dissipates"); Shaun B. Spencer, *Security vs. Privacy: Reframing the Debate*, 79 DENV. U. L. REV. 519, 519-20 (2002) (arguing that the trade offs between national security and privacy are often misrepresented in public discourse in ways that mistakenly make pursuing national security seem the more rational and more achievable path).

32. *See, e.g.*, Mike McIntire, *Ensnared by Error on Growing U.S. Watch List,* N.Y. TIMES, Apr. 6, 2010, at A1 (detailing two cases in which people who appear to pose no national security risk have been denied access to travel in ways that severely impinge on their careers, and noting the rapid pace of watch list expansion despite the frequent recurrence of such problems).

Overlisting also has institutional benefits. A large list of terrorist suspects suggests that terrorist activities are likely. That, in turn, suggests that more resources should be devoted to agencies that deal with terrorism. That cycle can encourage rent-seeking in the form of spurious prediction: a large watch list makes national security threats seem prevalent, which makes the agency's activities particularly necessary, which encourages attention and resources to flow to the agency and the watch list.[33] That encourages agencies to keep false positives—people incorrectly identified as terrorist threats—on their watch lists.

Of course, agents and agencies need not consciously decide to increase the number of false positives to bulk up watch list numbers. Rather, the rent-seeking opportunities may simply discourage agencies from spending the resources to develop assessment mechanisms that would reduce them.

B. *Relating False Positives to False Negatives*

One approach to terrorist watch lists holds that the increased number of false positives is a negligible price to pay. Any reduction in missed predictions, or false negatives, justifies any number of spurious predictions, or false positives. The point of a terrorist suspect database, after all, is to prevent terrorist attacks, not to prevent inaccurate listing. Inaccuracy, the argument goes, is a fine price to pay for the benefit of avoiding an attack, because the cost of allowing some very damaging events like terrorist attacks to occur will always be higher than the cost of inaccurate predictions.[34]

---

33. *Cf.* BERNARD E. HARCOURT, AGAINST PREDICTION: PROFILING, POLICING, AND PUNISHING IN AN ACTUARIAL AGE 27, 156 (2007). Harcourt argues that the practice of profiling leads law enforcement organizations to devote more resources to catching crime in the profiled population. *See id.* at 27. This skews public policy by creating a "self-fulfilling prophecy:" more crime is discovered within the profiled group because more resources are devoted to uncovering crime within it. *Id.* at 156.

34. *See, e.g.*, Richard Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 246 (2008); s*ee also* RON SUSKIND, THE ONE-PERCENT DOCTRINE: DEEP INSIDE AMERICA'S PURSUIT OF ITS ENEMIES SINCE 9/11, at 11-41 (2006) (describing this view). An analysis of the financial costs of the No Fly List estimates that taxpayers pay in the range of $100 million per year for that watch list alone. Marcus Holmes, *Just How Much Does that Cost, Anyway? An Analysis of the*

But whether, and when, that is the case is not clear. The always-worth-it view assumes a predictable trade-off between false positives and false negatives. Because including more names on a watch list means casting the net wider, having more false positives leads to having fewer false negatives. The model for this approach is the medical test that correctly recognizes a particular condition but is overly sensitive to its indicia. The medical test may mistakenly flag many people who have the indicia but do not have the condition, but at least it will also flag most people who have the condition. Its false positive rate assures a low number of false negatives.

A watch list with a protocol for predicting human conduct that effectively targets indicia of that conduct can present the trade-off in roughly the same form. But one with less carefully designed prediction protocols—or one that targets conduct whose indices are difficult to determine—may yield a high false positive rate without a correspondingly low false negative rate. Its predictions may simply be more arbitrary than recognition of symptoms by a medical test.

For instance, the terrorist watch list housed in the NCIC, the Violent Gang and Terrorist Organization File (VGTOF), asks agents to predict whether a person is likely to commit a terrorist act using a set of criteria developed to identify members of violent gangs. The FBI first developed a gang list in the early 1990s but expanded the list to include "terrorist organizations and members" after incoming Director Louis Freeh reevaluated the proposal.[35] Despite

---

Financial Costs and Benefits of the "No-Fly" List, 5 HOMELAND SEC. AFFAIRS 1, 2 (2009). In this Article, I focus on the nonmonetary costs that watch lists exact.

35. Minutes, National Crime Information Center Advisory Policy Board, Atlanta, Ga. 52 (Dec. 14-15, 1994) (document obtained through FOIA lawsuit) (Bates number NCIC-VGTOF-771) (on file with author). Taking up Director Freeh's suggestion, the Advisory Policy Board decided to "include terrorist organizations of an active and violent nature" within the definition of "gang." *Id.* Based on suggestions from the Department of Justice Criminal Division, this plan was revised to provide a freestanding definition for "terrorist organization" that was "in line with the definition commonly used by the FBI." *Id.* at 53. That definition describes terrorism as "activities that . . . involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State . . . [which] appear to be intended: (i) to intimidate or coerce a civilian population; (ii) to influence the

this new addition, the criteria for listing a terrorist remained the same as those for listing a gang member, "as [those criteria] apply to members of terrorist organizations."[36]

It is not clear, however, that the VGTOF's gang criteria are well suited to pick out terrorist conduct or likely terrorists. Specifically, the criteria for inclusion are either self-admission as a gang member upon arrest or incarceration, or two of the following: (1) identification "as a gang member by a reliable informant"; (2) identification "as a gang member by an informant whose information has been corroborated"; (3) "frequent[ing] a gang's area, associat[ing] with known members, and/or affect[ing] gang dress, tattoos, or hand signals"; (4) being "arrested multiple times with known gang members for offenses consistent with gang activity"; or (5) "[s]elf-admission" as a gang member at some point other than upon arrest or incarceration.[37]

Because the sociological characteristics of terrorist organizations differ from those of gangs, however, applying these criteria to terrorist suspects is not straightforward. The criteria may pick out gang-related conduct, but have little apparent relation to terrorist conduct. For instance, many American gangs occupy particular territory, often striving to control that territory in ways that mimic the control of the state.[38] But the United States has no

---

policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by [crimes] or kidnapping." 18 U.S.C. § 2331(1)(A)-(B) (2006); *see also* National Crime Information Center Advisory Policy Board; Meeting, 58 Fed. Reg. 27,752, 27,752 (May 11, 1993) (announcing that a "proposal for an NCIC Gang File" will be discussed at the Advisory Policy Board meeting to be held in June 1993); Notice of Lodging of a Consent Decree Pursuant to the Comprehensive Environmental Response, Compensation, and Liability Act, 58 Fed. Reg. 60,212, 60,212 (Nov. 15,1993) (announcing that that the "status of the NCIC Gang File" will be discussed at the meeting scheduled for that December).

36. *See* Privacy Act of 1974: Modified System of Records, 60 Fed. Reg. 19,774, 19,775 (Apr. 20, 1995) (specifying that the list would include identifying information of "[i]ndividuals about whom investigations has [*sic*] developed sufficient information to establish membership in a particular terrorist organization using the same criteria listed above [for gangs] as they apply to members of terrorist organizations rather than members of violent criminal gangs").

37. *Id.*

38. For example,

territories controlled by or associated with terrorist organizations in this way. Similarly, well-organized American gangs are known to often favor certain colors and clothes as external indicia of membership. In contrast, terrorists in the United States generally strive to remain hidden. It is thus unclear what kind of external indicia would serve as the terrorist version of gang colors, clothes, and signals.

The VGTOF criteria also give no indication of what constitutes a reliable informant or what kind of information would corroborate an informant's claim.[39] They do not specify who qualifies as a "known" terrorist organization member. If being listed in the VGTOF suffices to make someone a "known" terrorist, the vagueness of the list's criteria may simply reinforce itself. Moreover, precisely because the criteria are imprecise and subjective, one can imagine a range of views on what is required to fulfill them.

Despite these fairly obvious problems, neither the FBI's System of Records Notice nor internal documents produced in FOIA litigation have revealed an underlying theory that would explain how the VGTOF criteria would effectively pick out both gang members and terrorists. For instance, in 2002, "the military and other agencies" started "fingerprinting the detainees in Afghanistan, Pakistan,

---

> [B]y laying claim to certain 'turf' (i.e., by symbolically appropriating spaces, policing areas, and monitoring the behaviors of strangers) and offering services such as protection for residents, the gang effectively imposes onto [a] formal space a symbolic map that residents of the neighborhood are aware of and use to guide their own travels.

Sudhir Alladi Venkatesh, *The Social Organization of Street Gang Activity in an Urban Ghetto*, 103 AM. J. OF SOC. 82, 90-91 (1997). Venkatesh goes on to explain how individuals' movement through the area and through the city can be affected by the dominance of a gang in their neighborhood. Someone "visiting a friend" in another neighborhood "may minimize travel through those areas controlled by gangs that are at war with the one in his or her own neighborhood," and even a non-gang member visiting a loved one in an area or building controlled by a gang hostile to the one dominant in his neighborhood might need a special dispensation to be allowed to enter the building. *Id.* at 105. Some residents cease patronizing retail establishments and even social service providers in neighborhoods considered risky to travel to or enter because of gang affiliation. *See id.* at 106.

39. *See* TREVOR AARONSON, THE TERROR FACTORY: INSIDE THE FBI'S MANUFACTURED WAR ON TERRORISM 16-17 (2013) (arguing that many FBI informants have no reliable access to information on terrorism).

Cuba, and other places with those being sent to [the FBI] to . . . populate the [VGTOF]."[40] As is well known, however, the quality of American detention practices in the military operations following the 9/11 attacks left much to be desired: many detainees were victims of local political conflicts or false information, while others were in a sense sold for the high bounties offered by American forces.[41]

---

40. Minutes, Criminal Justice Information Services, Advisory Policy Board, Chicago, Ill. 7 (June 5-6, 2002) (Bates number NCIC-VGTOF-4269) (on file with author) (providing notes on speech by Michael Kirkpatrick, Assistant Dir. in Charge of the FBI's Criminal Justice Info. Servs. (CJIS) Division) (document obtained through FOIA lawsuit). Publicly available records do not indicate which two criteria such suspects fulfilled. It may well be that all of Afghanistan, for instance, was considered a terrorist organization "area," or that detainees were simply treated as presumptive terrorist suspects by virtue of being detained—despite the many known problems with identifying actual threats in areas of United States military activity.

41. *See, e.g.*, Ramzi Kassem, *From Altruists to Outlaws: The Criminalization of Traveling Islamic Volunteers*, 10 UCLA J. ISLAMIC & NEAR E. L. 85, 89 (2010–2011) ("Bounty leaflets were designed by various U.S. national security agencies and intelligence services and disseminated in Afghanistan after the invasion that followed the 9/11 attacks. . . . Many of the men who, like my clients, ended up in the U.S. military prisons at Bagram, Kandahar and Guantanamo were turned over for bounties similar to the ones offered in these leaflets, ranging from five to sometimes twenty thousand dollars, large amounts of money anywhere in the world but especially in countries with less affluent populations such as Pakistan and Afghanistan.") (citations omitted); Stuart Taylor, Jr., *Falsehoods About Guantanamo*, NAT'L J., Feb. 4, 2006, at 13-14 (reporting on a study that found that the best evidence suggests that fewer than 20% of Guantanamo detainees had been al-Qaeda members, that many were not members of the Taliban, and that most were handed over to United States forces by "reward-seeking Pakistanis and Afghan warlords and by villagers of highly doubtful reliability"); Mark Denbeaux et al., *Report on Guantanamo Detainees: A Profile of 517 Detainees Through Analysis of Department of Defense Data*, 2 (2006), http://law.shu.edu/news/guantanamo_report_final_2_08_06.pdf (finding that Defense Department data show that 55% of Guantanamo detainees had not been shown to have committed any acts hostile to the United States; that only 8% had been classified by the Defense Department as al-Qaeda members; that many had been detained based on very loose associations with groups that were not classified as terrorist organizations by the Department of Homeland Security; that most Guantanamo detainees had been handed over to United States forces by Pakistanis or Afghans at a time when the United States offered large bounties for suspected enemies); Tom Lasseter, *Day 1: America's Prison for Terrorists Often Held the Wrong Men*, MCCLATCHY (June 15, 2008), http://www.mcclatchydc.com/2008/06/15/38773/day-1-americas-prison-for-terrorists.html (reporting on a McClatchy investigation finding that dozens, and quite likely hundreds, of United States detainees in the War on Terrorism were

Without some empirical testing, we cannot know whether listing Afghan peasants who had run-ins with their neighbors or were turned over for the bounty also increased the chances that people who actually harbored terrorist intent would be listed as well.

Given all this, there is little reason to think that netting more false positives in the VGTOF will substantially reduce the number of false negatives. Because the VGTOF's criteria do not reliably pick out terrorist conduct or terrorists, the relationship between false positives and false negatives on the list will be much more arbitrary than that in a medical test that is overly sensitive to the symptoms of a disease. Without knowing the predictive protocol of a particular watch list, and without testing its efficacy, we simply cannot know how its false positive rate relates to its false negative rate.

Moreover, even in stark and highly salient areas like national security, it is not clear that the costs of *any* false negative will be high. Watch lists, after all, target potentialities. Given the practical difficulties of launching a terrorist attack, a person who is incorrectly identified as innocuous, despite having the propensity to commit a violent act, is still quite likely never to do so.[42] We cannot decide whether avoiding a false negative is worth some number of false positives without knowing more about both the likelihood of harm and its likely severity.

The always-worth-it view also ascribes astronomical costs to any false negative, and essentially zero costs to false positives. But false positives are not costless. For one thing, they decrease watch list efficacy because large numbers of irrelevant entries make it more difficult for users to distinguish signal from noise. Agents have a harder time identifying relevant, useful information that appropriately motivates action. It is well known, for instance, that government agencies had plenty of

---

"wrongfully imprisoned . . . on the basis of flimsy or fabricated evidence, old personal scores or bounty payments").

42. *See, e.g.*, AARONSON, *supra* note 39, at 19-34 (detailing the complexities of terrorist attacks and arguing that most terrorist plots in the United States since 2001 are creations of the FBI, because most people prosecuted for terrorist acts would not have been capable of planning or carrying out an attack themselves but depended to a large extent on conceptual, logistical, and financial assistance from the FBI through its confidential informants).

information indicating that the man who turned out to be the Christmas Day bomber likely posed a danger, yet he was allowed to board a plane.[43] The failure to spot and stop him earlier can be described as a failure of attention to relevant information. That information was lost in the mass of irrelevant information surrounding it.

More data also makes a database more difficult to maintain and increases data integrity, collection, maintenance, and protection problems. For instance, a Department of Defense (DOD) feasibility investigation recently concluded that creating a database of all Congressional Medal of Honor recipients—purely factual information in the government's sole possession—would impose such a serious administrative burden that it was "impracticable."[44] Maintaining information sufficient to predict human conduct, as watch lists do, clearly involves more data and difficulty than this purely factual compilation. If that easier task is impracticable, proliferating data on watch lists clearly poses a great challenge.

The agents and agencies that maintain watch lists work within a web of complex and often conflicting incentives. Because the predictive work that watch lists do is inherently uncertain and often difficult to test, direct incentives to individuals are difficult to design. Some scholars have proposed offering monetary rewards for good decisions in the administrative context.[45] But it is difficult to

---

43. THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, SUMMARY OF THE WHITE HOUSE REVIEW OF THE DECEMBER 25, 2009 ATTEMPTED TERRORIST ATTACK, 2 *available at* http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack (concluding that the intelligence community had sufficient information to know that Umar Farouk Abdulmutallab posed a danger but failed to "connect the dots"); Jeff Zeleny & Helene Cooper, *Obama: 'We Are at War'*, N.Y. TIMES: THE CAUCUS (Jan. 7, 2010, 4:53 PM), http://thecaucus.blogs.nytimes.com/2010/01/07/obama-review-revealed-significant-national-security-shortcomings/.

44. United States v. Alvarez, 132 S. Ct. 2537, 2551 (2012) (quoting "Brief for United States" at 55) (internal quotation marks omitted).

45. *See, e.g.*, M. Todd Henderson & Frederick Tung, *Paying Bank Examiners for Performance: Should Regulators Receive Bonuses for Effectively Guarding the Public Interest?*, 35 REG. 32, 32 (2012) (arguing that monetary bonuses linked to the value of regulated banks and timing of regulatory decisions would improve bank regulator performance by giving regulators a direct stake in the monetary value of their decisions).

implement a reward system in the absence of any mechanism for assessing judgment. Moreover, because watch list agents' subjective intuitions are constrained by watch list criteria and protocols, individualized incentives would put the burden on the wrong party. Where the agency has no way to test and update its predictive protocols, rewarding individual agents constrained by them will have only a small, and likely an arbitrary, effect.

Addressing agencies' perverse incentives and revising their assumptions about how false positives relate to false negatives, then, requires systemic regulation, not just individual rewards. Below, I propose requiring agencies to define what constitutes a false positive and a false negative, determine what levels of false positives and false negatives are acceptable, and assess and revise watch lists and their predictive protocols. To ground my proposals, I first introduce how watch lists work, emphasizing the key characteristics that differentiate them from other forms of knowledge and suspicion. I then describe the social and political effects that make them costly. Finally, I explain why current law does not suffice to constrain them.

II. WATCH LIST JUDGMENTS

In the dictionary and in the law, a database like a watch list is just an information repository.[46] In this view, the information in a database preexists its compilation. My bank account number, travel history, and marital status are facts just the same, whether they find their way to a database or not. But watch lists exceed this simple description. They not only compile independently existing

46. The Oxford English Dictionary defines a database as a "structured set of data held in computer storage and typically accessed or manipulated by means of specialized software," while Merriam-Webster defines it as "a usually large collection of data organized especially for rapid search and retrieval (as by a computer)." *See* OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/47411?redirectedFrom=database#eid (last visited Mar. 24, 2013); MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/database (last visited Mar. 24, 2013). The Privacy Act instead uses the term "system of records," defined as a "group of any records . . . from which information is retrieved by the name of the individual or by some . . . other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5) (2006).

information; they also contain predictions about how individuals will conduct themselves in the future.[47]

A. *Combinability, Portability, Decontextualization, Impersonality*

The information in watch lists is easily *combinable*, highly *portable*, relatively *decontextualized*, and largely *impersonal*. These things are in themselves not new: we have always been able to merge pieces of information, transfer information to new addressees, and scrub information of specificity. Still, networked information storage has made it easier for information in one database to be shared with new users, put to new uses, and combined with information from other sources. The amount of information that a modern database can hold and the ease with which that information can be transferred, manipulated, and combined is unprecedented—so much so that a difference in degree becomes indistinguishable from a difference in kind.

Increasing information collection and networking has gone along with forms of information input that enable easy *combination*. Narrative descriptions give way to predetermined information categories that can be harmonized across databases.[48] Networked databases with specific input fields can be combined with one another to yield ever more diverse information about individuals. Such

---

47. Bernard Cohn's classic study of British colonial knowledge production in India introduces the concept of an "investigative modalit[y]" to capture the activities that governments undertake to "classify, categorize, and bound the vast social world" they seek to control. *See* BERNARD S. COHN, COLONIALISM AND ITS FORMS OF KNOWLEDGE: THE BRITISH IN INDIA 5 (1996). "An investigative modality includes the definition of a body of information that is needed, the procedures by which appropriate knowledge is gathered, its ordering and classification, and then how it is transformed into usable forms such as published reports" and other evaluative conclusions. *Id.* Cohn's insights, developed to study colonialism, are broadly applicable to governments generally. Watch lists can be conceived as an investigative modality of the future.

48. *See, e.g.*, Richard V. Ericson & Kevin D. Haggerty, *The Policing of Risk*, *in* EMBRACING RISK: THE CHANGING CULTURE OF INSURANCE AND RESPONSIBILITY 239 (Tom Baker & Jonathan Simon eds., 2002) (describing, as an example, how Canadian police reports evolved from free-form narrative entries to forms with multiple fields requiring specific information, sometimes chosen from a limited range of choices).

combinations can also reveal previously unnoticed relations, similarities, and patterns through various processes loosely labeled "data mining."[49]

The same characteristics that make information easy to combine make it *portable*: easily distributed and understood beyond the circle of those who compiled or created it.[50] Combinability expands the scope of what information can reveal. Portability expands its audience—who it reveals things to. By making information accessible to potentially limitless addressees, networked databases like watch lists expand the uses to which information can be put and the situations in which it can be used: the packaging affects the product.

The information held in contemporary watch lists is relatively *decontextualized*, that is, easily removed from the conditions of its production. Users need not know much about the person at issue, the government agents who entered the information, how the criteria were developed, or how the information was compiled to be able to interpret a database's contents.[51] Decontextualization allows a database

---

49. Data mining can be defined as "the process of searching data for previously unknown patterns and using those patterns to predict future outcomes." Jonas & Harper, *supra* note 23, at 1. Jonas and Harper describe data mining as "a subset of the broader practice of data analysis," but note that "discussions of data mining have probably been hampered by lack of clarity about its meaning." *Id.* at 5.

50. *See* Paul Kockelman & Anya Bernstein, *Semiotic Technologies, Temporal Reckoning, and the Portability of Meaning. Or: Modern Modes of Temporality—Just How Abstract Are They?*, 12 ANTHROPOLOGICAL THEORY 320, 321 (2012) (defining portability as "a way of characterizing the degree to which" a way of producing meaning is or appears "widely applicable and/or contextually independent").

51. Decontextualization allows anyone familiar with the applicable symbolic system to understand information. It has been contrasted in a number of different realms of knowledge to information that requires more mutual knowledge, personal experience, or situation-specific understandings to be successfully understood. Indeed, that contrast has been seen as a central tension in modern knowledge-production. *See, e.g.*, EDWARD S. CASEY, THE FATE OF PLACE: A PHILOSOPHICAL HISTORY (1997) (discussing place and space); Martin Heidegger, *Modern Science, Metaphysics, and Mathematics*, *in* MARTIN HEIDEGGER: BASIC WRITINGS 305 (David Farrell Krell ed., 1993) (discussing modern science generally); Peter Galison, *Ten Problems in History and Philosophy of Science*, 99 ISIS 111, 119-22 (2008) (providing studies of scientific knowledge production). In that sense, terrorist watch lists partake of a larger trend of modern knowledge-production and its critique.

to look like a world unto itself: the information it contains appears independent of the world it describes.[52]

Similarly, watch list information appears *impersonal* because the way it is compiled and transmitted obscures its dependence on subjective judgment. Standardized forms calling for particular information and evaluative criteria presented as checklists give an objective feel to database information. Determining what criteria should underlie a prediction and whether a set of facts fit those criteria are themselves subjective, evaluative processes. But the personal judgment inherent in these determinations is masked by the impersonality of how databases collect and transmit them.

The combinable, portable, decontextualized, and seemingly impersonal information in a watch list is used to predict whether someone will likely commit a terrorist act in the future. Sometimes, that judgment comes from an individual agent's predictions about someone's conduct. Others offer predictions through automated processes based on algorithms that evaluate current behavior to predict future conduct. Those databases move subjective judgment from the direct evaluation of an individual by a person who makes a prediction to group evaluations made by those who develop the algorithm.

But in both cases, watch lists inscribe a governmentally authorized judgment about an individual. Unlike most forms of government judgment, though, they are subject to few legal constraints—as the novelty of granting standing to No Fly List plaintiffs indicates. Databases used in this way do more than simply compile information. They also create it.

---

52. Studies of language use link decontextualization of communicative signs with their entextualization elsewhere. Entextualization has been described as a "process of rendering discourse extractable, of making a stretch of linguistic production into a unit—a *text*—that can be lifted out of its interactional setting." Richard Bauman & Charles L. Briggs, *Poetics and Performance as Critical Perspectives on Language and Social Life*, 19 ANN. REV. ANTHROPOLOGY 59, 73 (1990). In this sense, a database prediction is "self-entextualiz[ing]"; it appears as a "formally autonomous totality" divorced from the communicators who created it. Michael Silverstein, *"Cultural" Concepts and the Language-Culture Nexus*, 45 CURRENT ANTHROPOLOGY 621, 626 (2004).

B. *The Division of Evaluative Labor*

Predictions made as part of database creation allow for a division of evaluative labor among numerous participants. Different people set the predictive criteria, make the prediction, validate it, and use it. For instance, the criteria for determining whether someone is likely to engage in a terrorist act comes from one division of the FBI.[53] Field agents then apply those criteria in individual cases, entering predictions that they submit to another agency division, which affirms the prediction based on field agents' entries.[54]

When nominating an individual who is not the subject of an ongoing FBI investigation for inclusion in the consolidated terrorist watch list, for instance, an FBI field officer submits the recommendation to an FBI Headquarters unit charged with reviewing the underlying information to determine whether it warrants passing on to the National Counterterrorism Center for inclusion.[55] Those predictions are then made available to all law enforcement agents in the country to guide their interactions with listed individuals.[56]

---

53. *See supra* note 20 and accompanying text; KROUSE, *supra* note 20, at 31-32; *see, e.g.*, Minutes, National Crime Information Center Advisory Policy Board, Atlanta, Ga., *supra* note 35, at 52 (recounting how the Violent Gang and Terrorist Organization File, an FBI gang and terrorist watch list, was developed by FBI working groups reviewing a Bureau of Alcohol, Tobacco, and Firearms proposal for a gang list); *see also* U.S. DEP'T OF JUST., OFFICE OF THE INSPECTOR GENERAL AUDIT DIV., AUDIT REPORT 09-25, THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES, at viii (May 2009), *available at* http://www.justice.gov/oig/reports/FBI/a0925/final.pdf [hereinafter TERRORIST WATCHLIST NOMINATION PRACTICES]; s*ee generally* Privacy Act of 1974; Modified System of Records, 60 Fed. Reg. 19,774, 19,774 (Apr. 20, 1995) (issuing a System of Records Notice for the VGTOF).

54. *See* TERRORIST WATCHLIST NOMINATION PRACTICES, *supra* note 53, at viii.

55. *Id.* at vii-viii. For nominations involving people who are subjects of FBI investigations, the intermediate review consists only of ascertaining that the documentation is complete and error-free. *Id.* For international terrorist suspect nominations, FBI headquarters first forwards the name on to the NCTC, whence it goes to the TSC. *Id.* An Inspector General report found that the mandated internal review was often not completed and that the "internal controls over these . . . processes are weak or nonexistent." *Id.* at xviii-xix.

56. *See The National Crime Information Center*, *supra* note 19.

The people who interact with the individuals listed in the database are, thus, far removed from the people who determined that the individuals should be listed in it. In the case of the VGTOF, for instance, officers who interact with suspects on the ground receive no information as to why a suspect ended up on the watch list: in 2009, the agency decided that the reasons a name was added to the list should not appear in the file.[57] Those who apply criteria to make predictions about listed individuals are, in turn, removed from those who decided what the criteria should be.

III. THE BROAD EFFECTS OF TERRORIST WATCH LISTS

Watch lists' combinability, portability, decontextualization, and impersonality, as well as their diffusion of evaluative labor, help differentiate them from other forms of knowledge production like individual, interpersonal determinations. These characteristics lend predictive government databases of all sorts both strengths and weaknesses. And they lead to broad individual, political, and social effects that are largely invisible when we think of watch lists as mere information repositories. This Part explores those larger effects, which comprise the hidden costs that watch lists exact.

A. *Effects on Agents and Agencies: Overconfidence and Skill Atrophy*

The diffusion of evaluative labor in watch lists leads to *cumulative* judgments that are produced by many individual participants at different stages of the predictive process. Like many database characteristics, cumulative judgment has both an upside and a downside.

By aggregating individual evaluations and judgments, accumulation can erase psychological peculiarities such as biases or other weaknesses in reasoning. Psychological research has recently tested experimentally what anthropology and sociology have always known: our evaluations of facts and people depend on our cultural

57. Minutes, CJIS Advisory Policy Board, National Harbor, Md. 24 (June 4-5, 2009) (document produced in FOIA litigation) (Bates No. NCIC-VGTOF-6100) (on file with author).

milieus.[58] World views, social connections, emotions, beliefs, and personal experiences affect people's judgments.[59] Doling out different parts of evaluation to different people may ameliorate some of these idiosyncratic psychological influences by diversifying the cultural milieus in play. And automating parts of the process may make it easier to spot the effects of cultural predispositions when they conflict with realistic assessments.

Moreover, removing evaluators from the uses of their evaluations may minimize some psychological impediments to improving database predictions. Experiments have repeatedly demonstrated that people tend to interpret new facts to accord with their existing convictions rather than allowing evidence that conflicts with their world view to alter it.[60] Because of this common phenomenon, people who make predictions may be averse to finding out whether they were right. Perhaps more importantly, they resist acting on evidence that they were wrong.[61] Separating those who make predictions from those who guide the criteria underlying predictions may alleviate some of those psychological obstacles. Those who devise criteria could learn from the mistakes of those who implement them rather than from their own mistakes.

At the same time, cumulative judgment can also undermine the efficacy of watch list predictions. Watch lists'

---

58. *See, e.g.*, Dan M. Kahan, *The Cognitively Illiberal State*, 60 STAN. L. REV. 115, 119-21 (2007).

59. *See, e.g.*, *id.*

60. *See, e.g.*, *id.* at 121 (citing Jonathan J. Koehler, *The Influence of Prior Beliefs on Scientific Judgments of Evidence Quality*, 56 ORG. BEHAV. & HUM. DECISION PROCESSES 28 (1993)) ("Real-world people tend to be anti-Bayesians: rather than update their prior beliefs based on new information, they tend to evaluate the persuasiveness of new information based on its conformity to their experience.").

61. Daniel Kahneman, a pioneer in the study of such irrationalities, has written about his own anti-Bayesian experience in the Israeli army, where he was on a team that assessed the leadership potential of army recruits. Feedback sessions regularly revealed that the team's "ability to predict performance . . . was negligible," but this "had no effects whatsoever on how we evaluated candidates and very little effect on the confidence we felt in our judgments and predictions . . . ." DANIEL KAHNEMAN, THINKING, FAST AND SLOW 209-11 (2011). Kahneman's subsequent research has shown that this "*illusion of validity*" is prevalent among those who make predictions. *Id.* at 211.

depersonalized nature gives them a veneer of objectivity that obscures the subjective, evaluative aspects of predicting individual conduct. The notion of objectivity has long teetered between indicating that a conclusion is true, on the one hand, and indicating that it is untainted by emotion or personal interest, on the other.[62] As historian of science Theodore Porter has pointed out, "[o]bjectivity as impersonality is often conflated with objectivity as truth."[63] The lack of an explicit subjectivity in database predictions—the absence of a visible person evaluating data and making predictions in a way that other participants can assess—contributes to the appearance of objectivity and encourages the conflation of impersonality with truth value.[64]

In other words, diffusion may ameliorate the effects of individual psychology by cancelling out biases, but it may also exacerbate them by obscuring individuality. Worse, it may lead to cumulative judgments that stack bias on bias. If people at different stages of the evaluative process share a world view and a cultural milieu, their agreement on a prediction can make it seem more reliable even when their evaluation merely compounds their individual prejudices or predispositions through ideological amplification.[65]

---

62. *See, e.g.*, Lorraine Daston, *Objectivity and the Escape from Perspective*, 22 SOC. STUD. OF SCI. 597, 597 (1992) (tracing the historical development of three conceptions of objectivity: "ontological objectivity," the pursuit of truth that revolves around "the fit between theory and the world"; "mechanical objectivity," the attempt to "suppress[] the universal human propensity to judge and aestheticize" by "forbid[ding] interpretation in reporting and picturing scientific results"; and "aperspectival objectivity," a related form that attempts to "eliminat[e] individual (or occasionally group) idiosyncrasies" by combining multiple approaches); Theodore M. Porter, *Quantification and the Accounting Ideal in Science*, 22 SOC. STUD. OF SCI. 633, 646 (1992) (arguing that the notion of objectivity, though sometimes equated simply with truth, is better understood as an ideal of "impersonality, standardization" that "reduc[es] subjectivity to a minimum").

63. THEODORE M. PORTER, TRUST IN NUMBERS: THE PURSUIT OF OBJECTIVITY IN SCIENCE AND PUBLIC LIFE 74 (1995). Porter argues that American public policy has historically been characterized by a tension between rhetorics of objectivity and the deployment of expertise. American government institutions have turned to "mechanical objectivity," a devotion to rule-based analysis, when their expertise was under attack. *See id.* at 4, 194.

64. *See id.* at 74.

65. *See, e.g.*, David Schkade, Cass R. Sunstein, & Reid Hastie, *What Happened on Deliberation Day?*, 95 CALIF. L. REV. 915, 917 (2007) (reporting

Moreover, the trend of federal agencies exempting watch lists from Privacy Act requirements and eschewing cost-benefit analysis for national security-related regulations, discussed above, suggests that even when evaluative labor is diffuse—and the psychological cost of being wrong is thus lowered—government actors often remain loath to assess their own predictive practices.

The diffusion of evaluative labor also helps decontextualize judgment. Judgment becomes "black box[ed]," looking ever less like evaluation and ever more like fact.[66] Involving computers in watch list predictions further intensifies black boxing: automation can obscure the very existence of decisions. In fact, however, automated evaluation is no less evaluative. Combining data from different sources, after all, requires some person to decide what kind of data to combine. And deriving knowledge from that combination requires someone to draw conclusions about its relevance and reliability. Data mining may reveal a pattern, in other words, but merely revealing a pattern is not enough. It still takes a person to determine whether that pattern is relevant to the problem that the watch list addresses.

In the networked world of watch lists, it is easy to treat information processing and combination as something computers, not people, do. Combining information from multiple databases to yield predictions is often seen, in Orin Kerr's words, as simply "data manipulation by a machine."[67]

---

experimental results showing that deliberations among groups of like-minded individuals led participants to take more extreme positions in a process of "*ideological amplification*"); Cass R. Sunstein, *Deliberative Trouble? Why Groups Go to Extremes*, 110 YALE L.J. 71, 118 (2000) ("[G]roup discussion is likely to shift judgments toward a more extreme point in the direction indicated by the median of predeliberation judgments.").

66. BRUNO LATOUR, SCIENCE IN ACTION: HOW TO FOLLOW SCIENTISTS AND ENGINEERS THROUGH SOCIETY 2-3 (1987) ("The word black box is used by cyberneticians whenever a piece of machinery or a set of commands is too complex. In its place they draw a little box about which they need to know nothing but its input and output."); *see also id.* at 253 ("The more . . . complex [machines] are, the more . . . each part hides the other as they become darker and darker black boxes.").

67. *See* Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, 11 BROOKINGS INST.: THE FUTURE OF THE CONST. SERIES 1, 4 (2011), http://www.brookings.edu/~/media/research/files/papers/2011/4/19%20surveillance%20laws%20kerr/0419_surveillance_law_kerr.pdf.

But that presents a somewhat idealized description of how information is processed. Machines do the aggregation, but people have to determine what to aggregate and how to aggregate it. People write the algorithms that machines perform and interpret the significance of any results. As Kerr's description shows, however, the role of people and their subjective judgments in these processes can be obscured by the higher visibility of machines and their seeming objectivity.[68]

The diffusion of evaluative labor also makes a database's predictions harder for any given participant to assess. Those who give predictions do not generally know how the criteria they apply were created and have no way of assessing whether those criteria effectively pick out the targeted conduct. Other participants similarly cannot assess the strengths of the predictions themselves. The separation of functions, of course, inheres in any organizational effort—division of labor has been recognized as a key aspect of complex institutions at least since Adam Smith. The inability of any participant to evaluate the overall effects of the predictive process is thus not surprising. It does, however, make it all the more important for organizations to have some means of assessing their predictive database uses.

The diffusion of evaluative labor can thus facilitate self-correction in some cases while facilitating its avoidance in others. It may be that certain areas are so emotionally laden and psychologically salient that diffusing evaluative labor does not suffice to ameliorate the psychological costs of being wrong.[69] It may also be that the politics surrounding high-salience areas makes self-assessment more difficult because it requires admitting our limited ability to protect against risk, and it introduces balancing requirements into areas that seem so urgent that balancing seems inappropriate.

For instance, when prediction depends heavily on agents' evaluations but appears to rest on objective criteria,

---

68. *See id.*

69. *See, e.g.*, Darryl K. Brown, *Cost-Benefit Analysis in Criminal Law*, 92 CALIF. L. REV. 323, 327 (2004) (noting that "a popular politics that . . . has tilted decisively toward harsh punitivism" has made introducing cost-benefit concepts into criminal law particularly difficult).

agents may come to misrecognize their own judgments as simple recognitions of fact. Over time, as agents accumulate more of these recognitions of fact, they may become prone to over-trusting their own judgments. With no external way to test whether their intuitions are correct, and no internal requirement to justify their conclusions, agents may come to feel that their evaluations are simply correct. But without any evaluation of their evaluations, we cannot know that they are.

Over time, this process will lead predictably to lowered standards of judgment: agents will feel increasingly justified acting on hunches or intuitions rather than requiring themselves to work through difficult, indeterminate reasoning processes that subject their own conclusions to doubt. The watch list they create will act as confirmation of their correct evaluation that an individual should be on the list. As long as every instance of judgment receives a positive response, judgment will appear very similar to fact.[70]

The evaluative processes that watch lists employ themselves form a part of their cultural milieu: they frame certain kinds of action as having predictive value, and they encourage different levels of self-reflection, self-doubt, and self-correction. How evaluation is structured in a database thus affects the assessment capabilities of the evaluators. If agents are never exposed to their mistakes or forced to reassess their instincts, they will make predictions under the illusion that they are generally correct. Moreover, feeble limits on false positives encourage agents not to examine the underlying premises of their decisions. That is, they encourage agents to have bad judgment.

The costs that the atrophy of judgment exact are tricky to calculate. While it seems clear that an unrealistic

70. A similar danger faces any agent with judgment responsibilities, of course. But the dangers seem to be starkest in high-salience areas like national security. For instance, a Senate report found that after an intelligence agent issued a report duplicating information available in major news outlets, a "performance review . . . cited this report as a signature accomplishment." S. PERMANENT SUBCOMM. ON INVESTIGATIONS, COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 41 (Comm. Print 2012), *available at* http://s3.documentcloud.org/documents/446657/fusion-centers.pdf. Praising people for imagining that public information constitutes an intelligence scoop seems unlikely to move them to improve their intelligence gathering abilities.

predisposition can damage an agent's ability to make accurate assessments, it is difficult to put a dollar value on that damage. And while it also seems clear that overvaluing the danger posed by terrorism can lead to a skewed distribution of government resources, it is hard to know just how much money or energy is misspent without knowing exactly how overvalued the dangers are.

B. *Effects on Governments: Simplification and Blinding*

Leaving watch lists unregulated not only lowers their efficacy. It also gives them undesirable power over the course of policy. As a seemingly neutral representation of reality, such predictions influence policymakers' views of their government's most urgent tasks. That influence can skew policy toward, or away from, particular problems by making the problems appear bigger or smaller.

Studies of government knowledge production related to complex, multicausal, dynamic processes have revealed that certain characteristics and problems typify them. Drawing on a range of work in social science and history, for instance, James Scott has examined how states engaged in a number of different projects have tried to take stock of, and control over, nature and society.[71] An underlying feature of such projects, Scott posits, is their reliance on "simplifications" that attribute particular importance to a few traits.[72] Those few traits come to define the entire object that the government seeks to control. Simplified descriptions make certain characteristics more salient and direct policy attention to them. In a sense, they reshape reality to make it more amenable to further, equally simplified, description.

Simplification makes labeling and tracking members of the relevant category easier. But it also inevitably ignores other attributes that may become important in their own right. Simplification also has its own recursive effect: it makes certain characteristics more salient, thereby

---

71. *See* JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED 2-4 (1998). The book discusses, for instance, the failures of collectivization in the Soviet Union, *see id.* at 193-222, compulsory settlement into villages in Tanzia, *see id.* at 223-61, and the attempt to order and plan forest growth in Germany, *see id.* at 281.

72. *See id.* at 81-82.

directing ever more attention to them. But it inevitably leaves out important characteristics of reality as well—characteristics that may not be relevant to some particular project, but that do not disappear simply because they are ignored. Government observation techniques similarly render people and entities more amenable to observation and control by emphasizing characteristics that are recognizable by those techniques.[73]

For Scott and others working in this vein, simplification, or attention to discrete characteristics, is not harmful in itself. Indeed, any representation of reality must reduce reality to some extent. Problems arise, rather, when governments take their own simplifications too seriously—when they refuse to acknowledge the simplifying relationship between the real and the represented.[74] As Andreas Glaeser has written, this is one of the "paradoxes of rational planning": planning depends on the "reification of particular representations," but reification itself "obfuscates the knowledge that representations are . . . operating in a realm different from what they represent," that is, that reality remains more complex and dynamic than its representation reveals.[75]

Giving too much credence to the representation thus impedes people's ability to grasp the more complex reality underlying it. A partial image not only stands in for the larger whole but also obscures the existence of that larger whole.[76] When states take their own simplifications too seriously, they forget that their categories are only provisional schema that highlight particular aspects of nature or society for particular purposes. They mistake their own simplifications for complete descriptions.

This misunderstanding is self-destructive: the state, fooled by its own seemingly perfect descriptions, is at the

---

73. *See id.* at 80-82.

74. *See id.* at 80.

75. Andreas Glaeser, *Monolithic Intentionality, Belonging, and the Production of State Paranoia: A View Through Stasi onto the Late GDR*, *in* OFF STAGE / ON DISPLAY: INTIMACY AND ETHNOGRAPHY IN THE AGE OF PUBLIC CULTURE 244, 245 (Andrew Shryock ed., 2004).

76. *Id.* (arguing that the representation becomes a kind of "fetish" through which "an aspectual translation is identified with the totality while knowledge of an underlying plurality is repressed").

mercy of all the unexpected, unexplored facts that it failed to take into account. And if the state has not built flexibility or correction into the system, it is powerless to modify its approach or react to unforeseen circumstances.

Of course, acknowledging a system's limitations from within the system is never easy. Timothy Mitchell's account of the natural and social problems that followed the building of the Aswan Dam, for instance, demonstrates the complexity involved: looking backward to explain how the dam project got started and how it affected its environment, his account connects everything from changing class relations in Egypt to the development of fertilizer out of munitions production, to the natural habitat of the mosquito, showing how each factor, and many others, played a small role in big events.[77] Mitchell argues that it was a lack of attention to the inherently multicausal nature of sociopolitical events—the illusion of complete knowledge to the exclusion of local practices that did not fit into the modernist paradigm of social and natural control—that led to the dam's problems.[78]

To see like a state, then, is to be a little bit blinded. The blinders are self-imposed: made of an eagerness to assume and a failure to doubt. We can always hope that acquiring more information will smooth out these obstacles through the law of large numbers. In the information age, it is inviting to assume that the mere availability of information itself provides the answers to difficult questions. But we cannot free ourselves so easily from reliance on judgment.[79]

---

77. TIMOTHY MITCHELL, RULE OF EXPERTS: EGYPT, TECHNO-POLITICS, MODERNITY 19-53 (2002).

78. Mitchell applies to the study of economics and politics the detail-oriented, interactional approach of Actor Network Theory, pioneered by Bruno Latour, which asks how the multiple factors that contribute to any phenomenon are interconnected into coherence. *See id.*; *see also* BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK-THEORY 1, 9-11, 21-25 (2007) (discussing Actor Network Theory).

79. The best known version of this understanding—that technical expertise cannot substitute for evaluation, and is to some extent dependent on it—was probably Weber's juxtaposition of formal rationality and value rationality. *See* ROGERS BRUBAKER, THE LIMITS OF RATIONALITY: AN ESSAY ON THE SOCIAL AND MORAL THOUGHT OF MAX WEBER 4 (1984) ("[W]hat is rational from one point of view may be non-rational or irrational from another," so that "[t]o the extent that people share ends and beliefs, they can agree in their judgments of

To become meaningful—to become knowledge—information must be interpreted.

This suggests that evaluations that are not continually examined for correspondence with reality will, with great likelihood, deviate from it. Without consistent attention to the relationship between the image and the world it represents—and without the assumption that any representation will leave out important factors—database prediction becomes less useful over time. But it also becomes more powerful. Watch lists tracking overlapping or redundant traits create the appearance of a proliferation of those traits—rather than a proliferation of watch lists.

C. *Effects on Society: Worldview and Urgency Mistakes*

Watch lists can have negative effects not only on agents, agencies, and governments, but also on society and policy more broadly. Scholars have amply demonstrated that government categorization profoundly affects both individuals' self-conception and their social status—the way others, including the government itself, conceive of them. The effects of any particular database use are difficult to pinpoint, of course, and their evaluative process often not susceptible to empirical observation. But a number of studies of similar or related processes provide a solid basis on which to work by analogy in considering how watch lists can affect more than the people who run them.

As numerous studies have shown, when governments and other powerful institutions create new social categories, "people . . . come to fit [those] categories" by reconceiving themselves in the categories' terms.[80] Perhaps the best

---

rationality and irrationality; but to the extent ends and beliefs diverge, so too will judgments of rationality and irrationality.").

80. Ian Hacking, *Making Up People*, *in* THE SCIENCE STUDIES READER 161 (Mario Biagioli ed., 1999). The full sentence is "[p]eople spontaneously come to fit their categories," but Hacking follows it with a demonstration of how such "spontaneity" depends on social, historical, and economic structures through which new categorizations are institutionalized. *See id.* at 161-69. To describe this process, which can involve both the introduction of a classification by "a community of experts who create a 'reality' that some people make their own" and "the autonomous behavior of the person so labeled, which . . . creat[es] a reality every expert must face," *id.* at 168, Hacking coins the term "dynamic nominalism": a dynamic nominalist approach holds "not that there was a kind of person who came increasingly to be recognized by bureaucrats or by students of

known scholar in this vein is still Michel Foucault, whose theoretical work drew attention to how the category of normal behavior leads individuals to reinterpret their own conduct and its relation to society.[81] Such studies have given empirical grounding to an insight vividly captured by Louis Althusser with the image of a person walking down the street when a policeman calls out, "[h]ey, you there!"[82] Without being named, the person stops and turns around.[83] He has been *interpellated*[84]—not just encompassed, but also defined and designated, by the state.[85]

Some of the clearest demonstrations of this defining power come in studies of mass categorization in which governments assign ethnic, religious, or hierarchical status to people based on a few characteristics like place of birth, kinship structure, or profession.[86] The individuals who are

---

human nature but rather that a kind of person came into being at the same time as the kind itself was being invented." *Id.* at 165.

81. MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan trans., 1979) (1975) [hereinafter FOUCAULT, DISCIPLINE AND PUNISH]; *see also* MICHEL FOUCAULT, MADNESS AND CIVILIZATION: A HISTORY OF INSANITY IN THE AGE OF REASON 38-64 (Richard Howard trans., Vintage Books 1st ed. 1973) (1961); IAN HACKING, REWRITING THE SOUL: MULTIPLE PERSONALITY AND THE SCIENCES OF MEMORY 21-38 (1998) [hereinafter HACKING, REWRITING THE SOUL] (describing the emergence of multiple personality disorder as a new self-description that was then taken up by people who fit themselves into this new category until it receded from both professional psychological and popular attention); IAN HACKING, THE TAMING OF CHANCE 1-3 (1990) [hereinafter HACKING, THE TAMING OF CHANCE] (describing the historical emergence of the science of statistics, as a way of determining normality in a quantifiable way).

82. LOUIS ALTHUSSER, *Ideology and Ideological State Apparatuses*, *in* LENIN AND PHILOSOPHY AND OTHER ESSAYS 174-75 (Ben Brewster trans., 1971).

83. *Id.*

84. *See id.*

85. The term interpellate puns on the combination of *interpolate* and *name* (*appeler* in French).

86. The Soviet government's anti-nationalist policy of "institutionalized multinationality," for instance, inscribed sub-state nationality—that is, a national belonging to one of the Soviet republics—in people's passports in an attempt to control mobility and defuse political opposition. *See* ROGERS BRUBAKER, NATIONALISM REFRAMED: NATIONHOOD AND THE NATIONAL QUESTION IN THE NEW EUROPE 23, 32 (1996). Brubaker shows how this policy, which aimed at creating unity among the Soviet republics, actually strengthened national identities. *See id.* at 32.

defined by these new categories may initially feel little connection to one another. Indeed, the new categories may seem somewhat arbitrarily assigned. But the very power of government definitions opens up room for those people to form groups—often politically important ones—on the basis of their shared identification with these categories.[87]

No less important is the way that others—such as governments themselves—come to view those who have been assigned to a category. Ian Haney López, for instance, has shown how case law on immigration status has helped mold social understandings of race in the United States.[88] Although a 1952 amendment eliminated race-based restrictions on naturalization, the jurisprudence that preceded the amendment helped shape the concept of race in America.[89] Because the opportunity to naturalize was granted primarily to free "white person[s]," and "persons of African nativity, or African descent,"[90] those who wished to naturalize were forced to frame their ethnicity in these governing terms, leading to a series of judicial opinions exploring, and cementing, particular notions of race.[91] The theory the Supreme Court settled on, Haney López shows, presented racial belonging as something easily visible to the naked eye—a restrictive notion of cultural and visual similarity.[92] This know-it-when-you-see-it understanding of race in the immigration context, Haney López argues, would have an enduring effect on American concepts of race generally. The immigration case law reinforced the concept of race as an inherent, obvious characteristic not subject to change over time, nor available to emendation due to new

87. For example, after the Chinese government consolidated a number of Muslim Chinese groups under the new catch-all category of Hui, the people so labeled came to use the classification as a unifying basis for pan-Hui political activism. *See* DRU C. GLADNEY, MUSLIM CHINESE: ETHNIC NATIONALISM IN THE PEOPLE'S REPUBLIC 6 (1996). Ian Hacking describes this process as the "looping effect of human kinds." *See* HACKING, REWRITING THE SOUL, *supra* note 81, at 21.

88. *See* IAN HANEY LÓPEZ, WHITE BY LAW: THE LEGAL CONSTRUCTION OF RACE 7, 12-13 (2006). Looking at medicine rather than law, Ian Hacking has analyzed how the recognition of multiple personality disorder led to its prevalence as a diagnosed condition. *See* HACKING, REWRITING THE SOUL, *supra* note 81, at 8-9.

89. HANEY LÓPEZ, *supra* note 88, at 33.

90. *Id.* at 31 (internal quotation marks omitted).

91. *See id.* at 35.

92. *See id.* at 64.

information about migration patterns, linguistic development, or other historical facts.[93]

Tracing a similar process in the colonial world, Bernard Cohn has shown that, although the Indian caste system appears to be an atavistic remnant of a premodern social system, it was largely created through the British colonial census.[94] That census recorded individual attributes that defined people in important ways, but that had always been assumed to be subject to change over time.[95] Census categories, in contrast, treated these attributes as unalterable signifiers of permanent social status.[96] It thus reified hierarchies that had previously been responsive to both social and biographical change.[97] Where caste had been an attribute of an individual at a certain time, the British census, which insisted that individuals be described in terms of its categories, made it into an eternal classification.[98]

Such research suggests that the categories of people that populate database predictions can affect broadly held conceptions of society. By creating categories of people and making them seem prevalent, or rare, watch lists can affect how both government actors and the public at large understand the composition of society. This accords with social psychological research indicating that people's assessments of risk depend on their cultural milieus, including on their own "group commitments" and the

---

93. *See id.* at 71-73.

94. *See* Bernard S. Cohn, *The Census, Social Structure, and Objectification in South Asia*, *in* AN ANTHROPOLOGIST AMONG THE HISTORIANS AND OTHER ESSAYS 230 (1987).

95. *See id.*

96. *See id.*

97. *See id.* at 230-31; *see also* COHN, COLONIALISM AND ITS FORMS OF KNOWLEDGE, *supra* note 47, at 8 ("[W]hat was entailed in the construction of the census . . . was the creation of social categories by which India was ordered for administrative purposes. The British assumed that the census reflected the basic sociological facts of India. This it did, but . . . the project also objectified social, cultural, and linguistic differences among the peoples of India[,] . . . le[ading] to the reification of India as [a] polity in which conflict . . . could only be controlled by the strong hand of the British.").

98. *See* Cohn, *The Census, Social Structure and Objectification in South Asia*, *supra* note 94, at 230.

opinions of others in their groups, as well the emotional valence of the conduct at issue for them and the ease with which they can imagine the risk coming to fruition.[99]

Changing how people think society looks can have multiple effects. It can lead agents and members of the public to more readily assume that someone is a terrorist because watch lists have already assured them that many people are terrorists. It can lead someone to interpret a particular pattern revealed by combining information from different databases as significant because the size of terrorist watch lists has already assured her of the significance of such patterns. It can lead local law enforcement officers and low-level agency administrators to pay more attention to those who are—or look like they might be—watch-listed in ways that distract them from other risks. And it can lead government agencies and legislatures to overstate the likelihood and the probable severity of the risks they deal with, skewing the distribution of limited government resources by channeling them to address low-probability events and to support low-efficacy programs.

Ironically, such effects are most likely in the very areas of high uncertainty that watch lists address. Government bodies that assess and understand the efficacy of their evaluative approaches can build that understanding into their predictions. They can, for instance, triangulate with external information, provide for regular reviews, or temper their reliance on evaluations in which they have less confidence. In contrast, where the government cannot, or will not, evaluate its own evaluative process, it cannot know how to modulate its reliance on its watch lists. This can make watch list evaluations less reliable without lessening the agency's reliance on them. On the contrary, a database whose predictive processes are not acknowledged can appear even more reliable than one whose pressure points are recognized.[100]

---

99. *See* Kahan, *supra* note 58, at 120.

100. *Cf.* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 721-24, 783 (2007) (arguing that the government monopoly over forensic methods—including their creation, testing, and execution—makes them particularly unreliable because they are subject to neither external oversight nor internal accountability checks).

The government as an institution has a pervasive power to shape social categories. Government databases like watch lists can thus affect how government agents and members of the public conceptualize their society and how they choose to distribute resources based on that conceptualization. That power can become dangerous when we forget that the image of society presented in database predictions is not a simple reflection of reality. Rather, it is a creature of our government. We should be able to discuss and assess not just the validity but also the desirability of imagining society in some particular way. But when we ignore the way that this image is created, we let the government off the normative hook.

IV. THE ABSENCE OF AN EFFECTIVE LEGAL REGIME

Many of the evaluations our government makes about us are constrained by a legal regime. Not only court judgments but many administrative conclusions must comport with the numerous requirements of due process and can be challenged if they fail to do so. Databases like watch lists, in contrast, are primarily governed by privacy law.[101] That law constrains how the government gathers information and, to a smaller extent, what kind of information it uses.[102] But it says little about evaluation, much less prediction. The predictive work performed in watch lists thus remains largely unregulated and unacknowledged by the law.

This might be acceptable if watch lists had negligible effects. And from a certain perspective, they do: being listed as a terrorist suspect does not constitute probable cause for arrest.[103] Yet watch listing clearly has effects on individuals.

---

101. *See* Cate, *supra* note 17, at 451 (documenting the scope of constitutional privacy protections for government database information); *id*. at 461 (discussing statutory provisions constraining government database information collection).

102. *See generally* 5 U.S.C. § 552a (2006).

103. According to a draft update, for instance, the NCIC Technical Operational Manual warns that a VGTOF "Group Member Capability" entry—that is, an individual listing on the watch list—does not constitute probable cause for arrest, search, or seizure, though it may form part of the probable cause inquiry. *See* National Crime Information Center; Technical and Operational Update, 9 (Nov. 7, 2005) (document produced in FOIA litigation) (NCIC-VGTOF-6891) (on file with author) ("[P]robable cause to search or seize is not established by the [VGTOF] record standing alone. . . . A caveat appears with every [VGTOF]

It can, as courts have begun to recognize, impinge on their right to travel.[104] It can also change individuals' status in the eyes of the law enforcement community, drawing extra scrutiny and suspicion. And although it cannot form the sole basis for probable cause, it can factor into a probable cause inquiry and a bail determination.[105] Moreover, as Part III demonstrated, watch lists have governmental, political, and social effects that far exceed their individual encumbrances.

In this broader frame, the absence of determinate legal consequences for the individual becomes only one concern. Government accountability, after all, accrues to all government actions, not just those with determinate legal consequences for individuals. Evaluating watch lists involves asking whether governments produce knowledge responsibly and accountably. As I show in this Part, current legal strictures, as well as scholarly analyses, skirt that crucial question.

A. *The Statutory Framework*

When Congress passed the Privacy Act in 1974, it knew it was dealing with something big. A Department of Health, Education, and Welfare (HEW) report had recently canvassed the unprecedented growth in government records about individuals, stressing the dangers it posed to a free society and proposing a number of "Fair Information

---

record warning against search or seizure established solely on the record. This does not mean that a [VGTOF] record has no relevance to either reasonable suspicion to investigatively detain a record subject . . . , to arrest a record subject based on probable cause, or to search premises or vehicles based on probable cause.").

104. *See supra* note 6 and accompanying text.

105. *See* United States v. Duque, No. CR-09-265-D, 2009 U.S. Dist. LEXIS 102199, at *13-14 (W.D. Okla. Nov. 2, 2009) (describing presence on the Violent Gang and Terrorist Organization File as part of "officers' collective knowledge," reasonably used to determine probable cause for an arrest); Ted Metzger & Ann O'Neill, *Protester Jailed, Denies He's a Terrorist*, CNN POLITICS (Sept. 6, 2012, 7:27 PM), http://www.cnn.com/2012/09/06/politics/protester-arrest-controversy/index.html (reporting that officer who arrested political protester for a minor traffic charge requested a judge to set bail at $10,000 and keep protester detained throughout a Democratic National Committee convention because the man was a "[k]nown activist + protester who is currently on a terrorist watch list").

Practices" to protect individual rights.[106] And a Congressional investigation headed by Senator Frank Church had yielded shocking revelations about the law enforcement community's incursions into political groups—the CoIntelPro activities that had disrupted lawful political activity, instigated violence through purposeful deception, and sought to discredit political activists by publicizing personal information about them.[107] The Congress that passed the Privacy Act was primarily concerned with two possibilities: information in government databases might be incorrect due to data integrity problems, mistakes, or purposeful falsehoods—and it might be used inappropriately as it was in the CoIntelPro operations.[108]

The growth of government records had occurred gradually and rather quietly. In 1909, for instance, Attorney General Charles Bonaparte testified to Congress that his Department had begun keeping records of "people who are actually in penitentiaries," but denied any interest in keeping records about those who had been only arrested, not convicted.[109] Ten years later, an unheralded report from

---

106. *Records, Computers, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems,* HHS PRIVACY COMM. (July 1973), http://aspe.hhs.gov/datacncl/privacy/ (last visited Mar. 23, 2013) (noting vastly increased government information maintenance about individuals, examining its actual and potential problems, and proposing information management principles).

107. *See, e.g.*, FRANK CHURCH, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. Rep. No. 94-755, at 1-20 (1976) [hereinafter Church Report].

108. *Cf.* at 314 (documenting abuses); *see generally* WARD CHURCHILL & JIM VANDER WALL, THE COINTELPRO PAPERS: DOCUMENTS FROM THE FBI'S SECRET WARS AGAINST DISSENT IN THE UNITED STATES (2d ed. 2002) (documenting abuses); WARD CHURCHILL & JIM VANDER WALL, AGENTS OF REPRESSION: THE FBI'S SECRET WARS AGAINST THE BLACK PANTHER PARTY AND THE AMERICAN INDIAN MOVEMENT (1988) (documenting abuses).

109. *The Prevention of Fraud in and Depredations Upon the Public Service: Hearing Before the H. Select Comm. on Appropriations*, 60th Cong. 424 (1909) (testimony of Charles Bonaparte, Attorney Gen. of the United States) (question by Congressman Fitzgerald). Attorney General Bonaparte noted that:

> Some persons have the idea that [collecting records of those arrested but not convicted] is of great value in the identification of criminals. How far that is well founded I am not prepared to express a positive

a special agent blithely noted just such an accounting, explaining that local law enforcement officials provided the federal government with finger prints and "records of arrest *or* conviction, as the case may be."[110]

As federal record keeping grew, Congress occasionally played catch-up to legalize practices that were already standard within the agencies.[111] But just as often, there was no Congressional action at all: keeping records about individuals was increasingly simply something agencies did.[112] Now, in the wake of the HEW report and the Church Committee revelations, that simple thing had become newly

---

> opinion. As far as our own records are concerned we merely take the records of the people who are at the federal penitentiaries.

Id. at 425. Similarly, the Attorney General's 1907 report to Congress describes the Department's "criminal identification records" as records of "persons convicted of crimes against the United States." ANNUAL REPORT OF THE ATTORNEY GENERAL OF THE UNITED STATES FOR THE YEAR 1907, H.R. DOC. NO. 10, at 44 (1907) (noting that these records "have been removed for preservation from the United States penitentiaries to the Department of Justice").

110. ANNUAL REPORT OF THE ATTORNEY GENERAL OF THE UNITED STATES FOR THE YEAR 1920, H.R. DOC. NO. 886, at 641 (1920) (Report of Special Agent A. J. Renoe) (emphasis added). By 1930, "[a]rrangements were effected whereby all United States marshals now submit to the division the fingerprints of all persons taken into custody by them." ANNUAL REPORT OF THE ATTORNEY GENERAL OF THE UNITED STATES FOR THE YEAR 1930, H.R. DOC. NO. 530, at 80 (1930).

111. For example, the FBI had been collecting criminal history records of some kind since the early part of the twentieth century. ANNUAL REPORT OF THE ATTORNEY GENERAL OF THE UNITED STATES FOR THE YEAR 1917, H.R. DOC. NO. 595, at 89 (1917) (under the heading of "Bureau of Criminal Identification"); ANNUAL REPORT OF THE ATTORNEY GENERAL OF THE UNITED STATES FOR THE YEAR 1911, H.R. DOC. NO. 117, at 22 (1911) (under the heading of "Bureau of Investigation"); H.R. DOC. NO. 10, *supra note* 109, at 44-45 (reporting criminal history record collection under the heading "Criminal Identification Records"). But it was not until 1930 that Congress officially recognized what the FBI was already doing by establishing a Division of Identification and Information charged with collecting "criminal identification and other crime records." Act of June 11, 1930, Pub. L. No. 71-337, 46 Stat. 554 (1930).

112. Agency information-collection activities in excess of statutory authorization appear, from this history, to be the norm rather than the exception. *See, e.g.*, Doe v. Immigration and Customs Enforcement, No. M-54(HB), 2004 WL 1469464 at *4 (S.D.N.Y. June 29, 2004) (holding that the inclusion of non-criminal immigration information in the NCIC, which the government claimed was mandatory, was in fact contrary to the statute authorizing the NCIC).

controversial. Like a mother startled to find an unruly adolescent where she had last seen a docile child, members of Congress felt pressed to take action: not just to catch up with agency practices but to control them.

Not surprisingly, they did so with a focus on individual rights. That is what the HEW report had worried about; that is what had been violated by CoIntelPro. While the Privacy Act went through numerous iterations and compromises, its central goal remained clear: to delineate and protect individuals' right to control the flow of information about themselves.[113] The preamble states that "[t]he privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies,"[114] and describes the act's purpose as "provid[ing] certain safeguards for an individual against an invasion of personal privacy."[115] At the same time, the act leaves largely unregulated the kind of information the government may collect about individuals.[116] Rather, it primarily controls how federal agencies gather, share, and store information about individuals.[117]

---

113. *See* STAFF OF S. COMM. ON GOV. OPERATIONS AND H.R. COMM. ON GOV. OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 2418 (PUBLIC LAW 93-579): SOURCE BOOK ON PRIVACY, VII (Comm. Print 1976); *see also* Alexi M. Poretz, *Disclosure Under the Privacy Act: A Matter of Interpretation*, 65 GEO. WASH. L. REV. 801, 802 (1997) (describing the Privacy Act as a measure that "safeguards individuals against the invasion of their personal privacy by restricting the manner in which federal agencies may collect, maintain, use, and disseminate certain personal information").

114. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, § 2(a) (1974).

115. *Id.* § 2(b).

116. The primary exception is that the act prohibits an agency from maintaining records "describing how any individual exercises rights guaranteed by the First Amendment." 5 U.S.C. § 552a(e)(7) (2006). But it exempts from this restriction records that are "pertinent to and within the scope of an authorized law enforcement activity." *Id.*

117. *See, e.g.*, Poretz, *supra* note 113, at 802 (1997) ("The Privacy Act of 1974 safeguards individuals against the invasion of their personal privacy by restricting the manner in which federal agencies may collect, maintain, use, and disseminate certain personal information."). The Privacy Act also applies in limited ways to organizations other than federal agencies. *See, e.g.*, 5 U.S.C. § 552a(a)(10)-(11), (*o*)(1). I do not address those applications here.

The Privacy Act relies mostly on external oversight: it gives people who are the subjects of agency records some knowledge about, and some control over, what those records say and how the information they hold is gathered, used, and distributed. The point is to limit agencies' control over information by forcing them to let individuals know how the information is being used and who else got to see it, as well as providing ways for people to see, contest, and correct their records.[118] The act also provides for some internal accountability, allowing agencies to collect only information that serves a specific legal purpose[119] and requiring them to ensure that information is relevant, timely, and accurate.[120]

As critics have noted, however, most of the powers that the Privacy Act takes away from agencies with one hand, it gives back with the other. Some provisions come with automatic exemptions. Agencies need not limit their distribution of records, for instance, if it falls within the stated "routine use" for which the information was collected—a use that the agency itself determines.[121]

---

118. For instance, the act requires agencies to publish and update notices in the Federal Register describing their databases, outlining the categories of records they hold and the categories of people they concern, and indicating the routine uses to which the records will be put. 5 U.S.C. § 552a(e)(4)(A)-(D) (requiring publication of System of Records Notices (SORN)). The act requires agencies to inform record subjects if their records will be distributed and seeks to limit the extent of that distribution. *Id.* § 552a(f)(1)-(4). It requires agencies to provide procedures for individuals to see and request the amendment of their own records, and allows for judicial review of an agency's refusal to do so. *See id.* § 552a(b). It requires each agency to establish a board to monitor its record storage procedures to ensure that the data are safe. *Id.* § 552a(u)(1)-(3).

119. *Id.* § 552a(e)(1).

120. *Id.* § 552a(e)(5). As a point of comparison, the Foreign Intelligence Surveillance Act (FISA) divides the database production process into the acquisition, retention, and use of information, with each stage subject to different requirements. *See* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 9:1 (2007). For instance, federal agents are required to "minimize" information disseminated to other parties, making retention and dissemination a complexly regulated decision. *Id.* At the same time, FISA minimization procedures primarily aim to protect the privacy of United States persons. *Id.* In this way, they mirror the concerns about privacy that I allude to. Despite more attention to how information is treated, then, FISA also does not address the classification issue per se.

121. *See* 5 U.S.C. § 552a(7), (b)(3). There are other exceptions on this limitation, such as distribution to the agency's own employees, for statistical purposes, or to save a life, but the routine use exception, as it is known, is

Agencies can also use other means to exempt their record systems from all but a few Privacy Act requirements.[122] The

probably the one that most undermines the original limitation. *Id.* § 552a(7), (b)(1), (4), (8); *see, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 136 (2004) (noting that the "routine use" exception is the broadest exception); Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 959-60 (1991) (noting that neither the executive nor Congress has not "actively overseen the exemption's use[,] [n]or has Congress deterred continued abuse of the exemption," and concluding that the breadth of the routine use exemption renders the act "impotent without more effective oversight"); John Shattuck, *In the Shadow of* 1984*: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 1003-04 (1984) ("All that is required to satisfy the . . . [Privacy] Act, the agencies say, is to publish each new computer-matching [i.e. data-mining] 'routine use' in the *Federal Register*."); *see also* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 695 (2007) (proposing that Congress eliminate the routine use exception, instead requiring agencies to "specify, up front, exactly how personal data will be used and under what conditions it will be transferred to other government agencies"). *But see* Major Lassus, *Routine Use Exception Under the Privacy Act of 1974 and the Requirement of Compatibility,* ARMY LAW., Nov. 1991, at 45, 50 (asserting that, despite being obscured by the "Act's convoluted evolution," the Privacy Act routine use exception actually "impose[s] two requirements for release of records under [the routine use exception]—namely, the procedural requirement of 'notice' and the substantive requirement of 'compatibility'" with the original "'purpose for which the information was collected'").

122. Some records can be exempted through the act's "General Exemptions" provision. 5 U.S.C. § 552a(j) (2006). This subsection exempts a system of records from all but a small number of Privacy Act provisions, specifically those that require that agencies limit extra-agency disclosure to people with a need for the record; keep an account on those to whom a record is disclosed; publish notices describing systems of records in the Federal Register (so-called SORNs); make reasonable efforts to ensure that a record distributed to someone *other than* an agency is accurate, timely, complete, and relevant; not keep records on individuals' exercise of their First Amendment rights unless a statute expressly authorizes it or the information collection falls within the scope of law enforcement activities; establish rules of conduct for people involved in database maintenance and creation; establish safeguards to ensure record security; and publish any new use of a system in the Federal Register with at least thirty days' opportunity for comment before implementing it. *See id.*; *see also id.* §552a(b), (c)(1)-(2), (e)(4)(A)-(F), (e)(6)-(7), (e)(9)-(11). Other databases, including those that hold "investigatory material compiled for law enforcement purposes [but not falling] within" the general exemption requirements, can be exempted from several specific provisions. *Id.* § 552a(k). This section allows for exemption from provisions that require agencies to make available to individuals who

Privacy Act thus inscribes a limited right to control information about oneself while giving agencies leeway to deviate from that ideal.

The Congress that passed the Privacy Act was concerned that government records could contain incorrect or false information and that information could be released in improper ways or for improper purposes.[123] In this conceptualization, the information at issue exists independently of, and prior to, its acquisition by the government. The information the Privacy Act is concerned with emanates from the individual, from whom the government must acquire it.

Commentators have long criticized the Privacy Act for insufficiently safeguarding individual rights and failing to update what safeguards exist to keep pace with technological developments.[124] But an even greater limitation is the act's understanding of databases and the work that they do. The Privacy Act treats databases as

---

request it an account of how their records have been disclosed to others; allow individuals to access, review, have a copy of, and request amendment of their records; acknowledge such requests for amendment and either implement them or explain a refusal to do so; allow individuals to file a statement of disagreement with the agency's decision and inform them of the availability of judicial review; note any such disagreement in subsequent dissemination of the record (except for information compiled in preparation for civil litigation); publish a system of records notice in the Federal Register that informs people how to find out if records pertain to them, access their records, and contest record contents, and that describes the categories of records in the system; and establish procedures to implement the notification, access, dispute and amendment provisions. *See id.*; *see also id.* § 552a(c)(3), (d), (e)(1), (e)(4)(G)-(I), (f). Aside from law enforcement databases, this exemption can also apply to records exempt from disclosure under the Freedom of Information Act's (FOIA's) national security exemption, 5 U.S.C. § 552(b)(1), and records "maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18." *Id.* § 552a(k)(3).

123. *See* Privacy Act of 1974 § 2(a), 88 Stat. at 1896.

124. *See, e.g.*, Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 138, 179 (2008) (arguing that U.S. privacy law's focus on data collection improperly overlooks important changes in data retention that changes how governments collect information and what information is available to them); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 877, 898 (2002-2003) (arguing that the United States lacks "well-established legal rights" of privacy, and new legal rights must be created to remedy policy violations); *see also supra* note 101 and accompanying text.

mere repositories for storing information. It regulates only the government's power to gather or use information. Watch lists, however, exceed those activities. They involve evaluating information and predicting future conduct—acts the Privacy Act does not address. This means that, while watch lists fall into the Privacy Act's bailiwick, they also fall through its cracks.

B. *The Doctrinal Context*

Courts have not laid out what process, if any, an agency must give a person it plans to put on a watch list. The No Fly List cases discussed in the Introduction will serve as test cases addressing that issue. But as this Article has suggested, those cases do not address the larger and more complex watch list infrastructure underlying the No Fly List itself.

Individuals, meanwhile, have found little recourse against agencies in this realm. For one thing, it is difficult to find out that one is watch-listed.[125] While someone denied boarding at an airport may infer that she is on the No Fly List, most individual repercussions of watch listing are more discreet. They come in the form of heightened attention from law enforcement agents[126] and others given

125. *See, e.g.*, El Badrawi v. Dep't of Homeland Sec., 583 F. Supp. 2d 285, 295-96 (D. Conn. 2008) (explaining that, in accordance with its policy, the FBI "refuses to confirm or deny" the existence of VGTOF records responsive to a Freedom of Information Act request).

126. For instance, an officer who queries the NCIC for a name that is listed in the VGTOF may be instructed by the VGTOF text to "APPROACH WITH CAUTION" and "DETAIN THIS INDIVIDUAL FOR A REASONABLE AMOUNT OF TIME FOR QUESTIONING" because the "INDIVIDUAL IS OF INVESTIGATIVE INTEREST TO LAW ENFORCEMENT REGARDING ASSOCIATION WITH TERRORISM"; the officer will likely be instructed to also "IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER." National Crime Information Center; Technical and Operational Update, 13 (Nov. 7, 2005) (document produced in FOIA litigation) (NCIC-VGTOF-6895) (on file with author). The officer may receive slightly different instructions depending on how the individual is listed, but in every case the implication is that the officer should pay particularly careful attention to the individual. *See id.* 13-14 (NCIC-VGTOF-6895-96) ("ASK PROBING QUESTIONS TO DETERMINE IF THIS INDIVIDUAL IS IDENTICAL TO THE PERSON OF LAW ENFORCEMENT INTEREST. . . . APPROACH WITH CAUTION. . . . DO NOT ADVISE THIS INDIVIDUAL THAT THEY ARE ON A TERRORIST WATCHLIST."). While there have been no studies so far of exactly how watch

access to watch list entries, which may include private institutions and non-law enforcement governmental entities.[127] Agencies do not disclose watch list status to the individual.[128]

Even if a person is able to discover that she is on a watch list, she has few avenues of action available. In the 1970s, a line of case law in the D.C. Circuit held that statutes authorizing law enforcement databases themselves provide an avenue of redress for people listed incorrectly.[129] Another line of cases holds that, even absent a statutory cause of action, courts have inherent equitable authority to expunge government records about individuals.[130] That reasoning was used to expunge arrest records when the arrests were found to have been without probable cause and for unconstitutional purposes, or when the laws underlying

---

lists affect the exercise of law enforcement agent discretion, scholarship has demonstrated that law enforcement officers tend to give increased scrutiny to people with arrest records even in the absence of subsequent charges or convictions. Note, *The Impact of Arrest Records on the Exercise of Police Discretion*, 47 LAW & CONTEMP. PROBS. 287, 295-98 (1984) (detailing how, despite the absence of a necessary relation between arrest records and past criminality and a lack of evidence that arrest records function as useful predictors of future criminality, arrest records significantly affect the exercise of police discretion). It is likely that terrorist watch list entries have similar effects on discretion, especially since the watch list itself instructs officers to increase their level of scrutiny.

127. *See* 28 C.F.R. § 50.12(a) (2012) (authorizing the FBI to share NCIC records with banks, "certain segments of the securities industry," "registered futures associations," "nuclear power plants," and "state and local governments for the purposes of employment and licensing").

128. *See, e.g.*, El Badrawi v. Dep't of Homeland Sec., 258 F.R.D. 198, 205 (D. Conn. 2009) (asserting that the FBI "properly refused to confirm or deny whether [an individual] was listed in the VGTOF" in a Freedom of Information Act (FOIA) case, but noting that the balance of interests was different in civil litigation discovery).

129. *See* Tarlton v. Saxbe, 507 F.2d 1116, 1122-23 (D.C. Cir. 1974) (holding that the statute authorizing the FBI to collect criminal identity information implicitly required the FBI to take "reasonable precautions to prevent inaccuracy"); Menard v. Saxbe, 498 F.2d 1017, 1028-29 (D.C. Cir. 1974) (holding that the statute authorizing the NCIC impliedly provided a remedy for someone contesting a record of an arrest that lacked probable cause because the FBI had an affirmative duty to maintain accurate criminal identification files).

130. *See Menard*, 498 F.2d at 1025.

the arrests have been found to be unconstitutional.[131] But as the Supreme Court moved away from implied rights of action over the following decades,[132] these lines of reasoning grew fallow.[133] Moreover, the passage of the Privacy Act in 1974 appeared to provide a statutory avenue of redress even though, as discussed in the previous Section, it provides redress only for inaccurate reporting of existing information—not for spurious predictions or mistaken evaluations.[134] Indeed, precisely because of the subjective and often vague criteria for inclusion in a watch list—not to mention their secrecy—it is difficult to contest watch listing on the grounds of inaccuracy.

The Administrative Procedure Act's (APA) grant of judicial review to "person[s] . . . adversely affected or aggrieved by agency action" is also of limited use in the watch list context.[135] The adverse effects of watch listing on an individual include higher scrutiny from a law enforcement officer, prospective employer, and others.[136] Such increased scrutiny has been shown to influence the exercise of discretion. Even arrest records with no subsequent records of conviction, which have not been shown to predict future criminal behavior, influence law enforcement agent behavior with respect to suspects.[137] Given the heightened state of terrorism fear that has characterized American law enforcement since the terrorist attacks of 2001, it is safe to conjecture that being on a

---

131. *Id.*

132. *See* Cort v. Ash, 422 U.S. 66, 78 (1975) (placing strict limits on a court's ability to imply a private right of action based on general government responsibilities absent a specific statutory grant).

133. *See, e.g.*, *El Badrawi*, 579 F. Supp. 2d at 279-80 (declining to infer a cause of action in the statute authorizing the FBI to collect criminal information because the statute did not explicitly waive sovereign immunity).

134. *See* discussion *supra* Part IV.A.

135. Administrative Procedure Act, 5 U.S.C. § 702 (2006).

136. *See supra* notes 126-27 and accompanying text.

137. *The Impact of Arrest Records on the Exercise of Police Discretion*, *supra* note 126, at 295-98; *see also* Herman Goldstein, *Confronting the Complexity of the Policing Function*, *in* DISCRETION IN CRIMINAL JUSTICE: THE TENSION BETWEEN INDIVIDUALIZATION AND UNIFORMITY 23, 33-34 (Lloyd E. Ohlin & Frank J. Remington eds., 1993); H. Richard Uviller, *The Unworthy Victim: Police Discretion in the Credibility Call*, 47 LAW & CONTEMP. PROBS. 15, 28 (1984).

terrorist watch list will have serious effects on an individual's interaction with government agents. Indeed, as Seth Kreimer has written, "the discretion of the modern administrative state is well adapted to low visibility retaliation," in which lists ostensibly compiled for law enforcement purposes can end up being used as tools for selective prosecution or auditing.[138] Moreover, the very knowledge that one may be the object of government scrutiny can itself inhibit otherwise licit activities.[139]

Nonetheless, such aggrievement is difficult to cognize in court because it is difficult to pinpoint an actual or imminent concrete harm, as required for standing.[140] Whether a court will interpret the predictable effects of watch listing as an imminent threat depends as much on the judge's view of standing as on the actual effects of watch listing. And many adverse effects of watch listing, such as visa refusals for foreign nationals, are simply discretionary and not subject to judicial review.[141] A court will not find aggrievement where a person has no right to any particular outcome.

Someone who can demonstrate standing should in principle have access to judicial review of his watch list status under the APA. But even in that situation, a plaintiff will face an uphill battle. The APA precludes relief when "any other statute that [waives sovereign immunity] expressly or impliedly forbids the relief which is sought."[142] If the watch list has been exempted from Privacy Act requirements, as all terrorists watch lists have, the APA provision may render any form of relief under the Privacy Act unavailable, because the exemption prevents relief.

---

138. Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133, 150 (2004).

139. *Id.* at 155 ("Fear or suspicion that one's speech is being monitored . . ., even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.") (quoting Bartnicki v. Vopper, 532 U.S. 514, 533 (2001)).

140. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

141. *See, e.g.*, Am. Acad. of Religion v. Napolitano, 573 F.3d 115, 123-24 (2d Cir. 2009) (discussing the doctrine of "consular unreviewability," which bars judicial review of visa issuance or refusal except in limited circumstances).

142. Administrative Procedure Act, 5 U.S.C. § 702 (2006).

As the recent No Fly List cases demonstrate, there is one avenue left to a prospective plaintiff: to sue to expunge—rather than correct—the record, or for additional process in contesting its existence. Those forms of relief are not available under the Privacy Act and therefore not precluded by exemption from it.[143] Still, as the novelty of these cases illustrates, it is only the rare plaintiff who can fulfill the requirements necessary to sustain a suit. The real problem, though, as I discuss in the following section, is that litigation is simply not well suited to address systemic problems in agency functioning.

C. *The Privacy Paradigm and the Language of Litigation*

Scholarship on watch lists shares the legal regime's predilections. Scholars writing about government databases generally tend to focus on the way individual privacy rights bump up against the needs of the nation.[144] Like the law, the literature tends to elide the evaluation and prediction that go into making a watch list.

Like the law, scholars focus on individual privacy,[145] specifically, what is known as information or data privacy.[146]

---

143. Even in such a case, at least one court has concluded that sovereign immunity bars the suit. Badrawi v. Dep't of Homeland Sec., 579 F. Supp. 2d 249, 279-80 (D. Conn. 2008). Although the *Badrawi* court did not make clear how the APA figured in its determination, the implication is that it did not see the plaintiff as having been "adversely affected or aggrieved by agency action," which is required for the APA's waiver of sovereign immunity. *See* Administrative Procedure Act § 702.

144. *See* Shattuck, *supra* note 121, at 992 (concluding that including "information about the non-criminal activities of persons under surveillance by the Secret Service" in the National Crime Information Center database clearly violates basic privacy rights); Spencer, *supra* note 31, at 519 (arguing that presenting database use as a privacy-security trade-off encourages valuing security over privacy by "fail[ing] to account for the many unintended consequences that usually flow from security measures" and presenting security benefits as unrealistically tangible and certain while presenting privacy harms as unrealistically abstract and hypothetical); *compare, e.g.*, Soma, *supra* note 31, at 287 ("[H]istorically, a return to equilibrium has occurred as the initial threat dissipates."), *with* Vern Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEX. L. REV. 837, 838 (1971).

145. Scholars have been at pains to find something that unifies the diverse areas to which American law has applied the label of privacy. Jerry Kang has posited that there are three kinds of privacy rights in American law that assure individuals decisional (personal choices), spatial (physical sphere), and

Some commentators working in this vein stress the psychological importance of information privacy in constituting individual identities.[147] They argue that data collection impinges on the construction and expression of the self[148] and exacerbates power inequalities between the surveilling agent and the surveilled subject.[149] They also

---

informational (personal information) control. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-05 (1998). This typology covers the areas that United States law sees as implicating privacy, but does not suggest an underlying concept uniting the typological components—perhaps reflecting the lack of underlying logic connecting the arenas that United States law has labeled private. While accurately depicting the legal distribution of privacy, this typology also emphasizes that the American legal conception of privacy rests on doctrinal development and political history, not on the recognition of an independent entity in the natural or the social world.

146. *See, e.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (2006).

147. Some scholars worry that information-gathering about individuals impinges on the construction and the expression of individuality itself. They posit that being observed—either physically or informationally—imposes a kind of chilling effect on conduct, constraining how people feel they can act and therefore who they can be. Such writers investigate how surveillance can organize situations in ways that affect how people behave, and how people feel they *can* behave. *See, e.g.*, Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 194 (2008) (describing surveillance as constricting "the parameters of evolving subjectivity" and limiting how particular spaces can "function as contexts within which identity is developed and performed"); Luciano Floridi, *The Ontological Interpretation of Informational Privacy*, 7 ETHICS & INFO. TECH. 185, 195 (2005) (positing that persons are constituted by their personal information and interpreting information privacy as a protection of personal identity); *see generally* FOUCAULT, DISCIPLINE AND PUNISH, *supra* note 81, at 125-31 (describing the increased surveillance practices of modern institutions as regimenting and evaluating individuals according to a norm that is presented as universally applicable in ways that constrict individual behavior even absent direct coercion).

148. *See, e.g.*, Kirstie Ball & Frank Webster, *The Intensification of Surveillance*, *in* THE INTENSIFICATION OF SURVEILLANCE: CRIME, TERRORISM AND WARFARE IN THE INFORMATION AGE 1, 13-14 (Kirstie Ball & Frank Webster eds., 2003) (identifying one problem with information-gathering about individuals as the inevitably partial quality of the knowledge garnered, which gives the surveillor access to the individual's actions but not his motivations or his real inner self).

149. *See, e.g.*, *id.* at 14 (positing that one problem with increased surveillance is the fact that observers, who "are frequently not known to the subject," can use

show how data collection can threaten the very possibility of community by violating the interactional patterns that weave communities together, making membership more perilous and therefore less likely.[150] Others emphasize the legal importance of allowing people to keep information secret or make it accurate, arguing that due process and privacy rights are at stake in the government's collection of individual information.[151] Still others focus on the paucity of

---

their surveillance for ends the subject does not know about, even though "to garner information for disguised purposes is morally dubious").

150. *See, e.g.*, Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137 (2004) (suggesting that each sphere of social life is governed by "norms of information flow" that define the kinds of information exchange appropriate to that context and determine what counts as privacy in that context); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989) (proposing that the concept of privacy "safeguards [the] rules of civility that . . . constitute both individuals and community"); *see also* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 974 (2005) (suggesting that whether someone has a reasonable expectation of privacy in a given context should depend on how information usually travels in that particular context). Daniel Solove, a prominent privacy scholar, has described American thought on privacy as comprising six primary strands or approaches. While Solove is concerned to point out their differences, it turns out that each of the six centers on the kinds of individual rights issues discussed above: control over information about the individual and the individual's ability to constitute himself within his community. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 12-34 (2008). These strands of thought see privacy as: 1) a right to insist on "seclusion," *id.* at 18; 2) an ability to "conceal[]" or limit access to the individual, *id.*; 3) a right to secrecy, *id.* at 21; 4) control over the flow of information about one's person, *id.* at 25; 5) freedom from the objectifying effects of surveillance, which intrudes on the aspects of personhood, selfhood, or subjectivity that inheres in limiting the flow of information about one's person, *id.* at 29; and 6) a prerequisite for intimate relationships and other kinds self- and community-constitution that depend on interpersonal motivations and choices, *id.* at 34. Similarly, Solove's own book-length study of public and private databases focuses on problems involving the gathering, maintenance, and dissemination of individual information, like people's inability to correct mistakes in database records, the government's tendency to collect information that it does not need or ought not have, the lack of legal protection afforded information voluntarily revealed to third parties, and the difficulty of keeping data secure. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2-8 (2004).

151. *See, e.g.*, Jonathan C. Bond, Note, *Defining Disclosure in a Digital Age: Updating the Privacy Act for the Twenty-First Century*, 76 GEO. WASH. L. REV. 1232, 1237 (2008) (arguing that the Privacy Act should be amended to further protect private information from disclosure); Shaina N. Elias, Essay, *Challenges*

privacy protections in American law and on the technological and legal trends that threaten the protections that do exist.[152]

Some scholars working on databases generally do recognize that surveillance affects not just individuals, but

---

to Inclusion on the "No-Fly List" Should Fly in District Court: Considering the Jurisdictional Implications of Administrative Agency Structure, 77 GEO. WASH. L. REV. 1015, 1032 (2009) (urging courts to interpret statutes so as to give travelers a way to challenge inclusion on such lists); Justin Florence, Note, *Making the No Fly List Fly: A Due Process Model for Terrorist Watchlists*, 115 YALE L.J. 2148, 2165-81 (2006) (urging agencies to adopt procedures that respect people's right to have notice and an opportunity to heard on their status); *see also* Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring) (positing that the Fourth Amendment protects arenas in which an individual has a "reasonable expectation of privacy"); Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 913-16 (2002) (arguing that privacy practices affect privacy rights, insofar as increasing government data collection conditions people to expect fewer rights and less privacy to begin with).

152. *See, e.g.*, Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 610 (2007) ("The dangers of any large-scale government effort to collect, catalogue, and manipulate information on individuals are never far-fetched."). Bignami urges the United States to move toward a privacy regime more closely aligned with the more stringent laws of the major European countries, which recognize individual information privacy as a fundamental right; strictly limit private entity data collection and retention; require that government data-collection be specifically authorized by statutes and subject to proportionality review; and enforce privacy rights through a dedicated, independent agency. *Id.* at 635-36, 653. Others warn that legal restrictions on government information-gathering have not kept pace with technological developments that allow for less legally encumbered, but more effective, government information gathering. *See, e.g.*, Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 138 (2008). Bellia notes that U.S. privacy law restricts the government's "collection and disclosure of certain kinds of information," but leaves the *retention* of information virtually unregulated. *Id.* Because the collection and retention of data by private parties, such as service providers, is also largely unregulated in the United States, Bellia argues, government agencies can effectively circumvent legal strictures on real-time surveillance by simply collecting retained data from private third party providers. *Id.* at 140. This is facilitated not only by the relatively lax regulation of private parties, but by technological developments that have rendered third-party data retention increasingly cost-less and ubiquitous. *Id.* Bellia urges legal reforms to ameliorate the "surveillance-enhancing effects" of this new "architecture of memory" in which little is forgotten. *Id.*

entire societies.[153] And some have noted that databases not only collect information about individuals but provide models on which to "*make inferences*" about how those individuals will behave—specifically, how they will spend money.[154] Even this literature, however, generally skips straight to effects on the individual: it does not ask how those who work with databases form their predictions.

This literature also tends to assume that information gathering is always pernicious. This may be why, for this approach, the difference between good and bad predictions is not really that important: each is morally repulsive in its own way.[155] Bad predictions show that information gathering yields only a partial picture, because economistic models can never capture the intricate complexity of individual identity. Good predictions instantiate the harms of surveillance, showing how it constricts free will and individuality in ways that impinge on our very humanity.

Whatever the value of this assumption in the private sphere,[156] it is less tenable in the public law arena, where

---

153. *See, e.g.*, Ball & Webster, *supra* note 148, at 12; David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, *in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION 13, 16-17 (David Lyon ed., 2003).

154. OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 53 (1993) (quoting KLAUS KRIPPENDORFF, CONTENT ANALYSIS 37 (1980)) (internal quotation marks omitted). Gandy generally discusses how private parties gather and organize information about individuals to sort them by economic roles and proclivities, thus "reduc[ing] . . . uncertainty about individual behavior" in ways that have become "central" to capitalism. *Id.* at 45; *see id.* at 1 (calling this process "the difference machine that guides the global capitalist system"). Scholars have noted that such predictions themselves affect economic conduct by constraining the available kinds of money-spending opportunities that people are presented with. People's incomes determine the kind of marketing they receive; their credit histories determine the amount of credit they are offered; their medical symptoms influence the cost of their health insurance. *See* Lyon, *supra* note 153, at 14, 21, 27.

155. Gandy, for instance, asserts that economic sorting systems are "based on theoretical models that reflect quite transitory fads or trends in social, economic, and political thought," GANDY, *supra* note 154, at 2-3. But he also warns that the mechanism's "methods are constantly being adjusted as" their conclusions "are evaluated in terms of their contribution to the realization of the organization's goals," which suggests increasing accuracy over time. *Id.* at 55.

156. In the private, economic arena, such studies tend to frame information practices as pitting corporations and their profit motives against individuals

both the harms and the benefits of watch lists redound on the same society.[157] Different evaluative approaches and the difference between good and bad predictions should matter to the analysis of government databases, which implicate questions of government conduct and resource distribution as well as national well-being.

The literature's focus on individual rights, which mirrors the values inscribed in the Privacy Act, fits comfortably into the more general study of privacy in the United States, which from its start has been animated by a concern with the collection and dissemination of information.[158] It also goes along with a search for individual remedies, usually phrased in the language of litigation.[159] This makes sense: our system presents individual rights as vindicated primarily through courts and court-like proceedings.[160] The normal concerns of courts—like whether

---

and their nonprofit communities. *See, e.g.*, Lyon, *supra* note 153, at 14. Even in the private sphere, however, arguments can be made for the benefits of accurate market categorization: one person's higher interest rate might result in another's easier access to credit.

157. Indeed, the goal of many predictive government databases is precisely to constrain individual freedom—for instance to engage in violent behavior—to benefit society at large.

158. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197-214 (1890). The beginning of American privacy law is usually dated to a well-known 1890 article in which Samuel Warren and Louis Brandeis first posited that the law protected a right to individual privacy. *See id.* By this they meant that the individual had a kind of authorial right, as the creator of the news or image in which he figured, to decide whether it should be made public. *Id.* at 204. At the same time, for Warren and Brandeis this kind of control was superior to a mere right to intellectual property. It instantiated a "more general right . . . to be let alone," or, more grandiosely, a right to one's own "inviolate personality." *Id.* at 205. The authors thus proposed to limit the personal information available to other people. *Id.* at 214-20. They did not discuss what people *do* with the personal information they get. That evaluative step has largely lurked in the background of scholarship on privacy and, by extension, on government databases.

159. For instance, commentators consider how individuals can contest inclusion in a database through court or court-like processes. *See, e.g.*, Elias, *supra* note 151, at 1017, 1029-32 (urging courts to interpret statutes so as to give travelers a way to challenge inclusion on such lists); Florence, *supra* note 151, at 2180-81 (urging agencies to adopt procedures that respect people's right to have notice and an opportunity to heard on their status).

160. The orientation toward litigation, based on a concern with individual rights, is not confined to the arena of databases or of privacy. Robert Kagan has,

including information in a database imposes harms sufficient to support standing—naturally come into play.

But asking whether someone has suffered standing-worthy harm helps us analyze only the propriety of bringing certain issues to court. It does not help us analyze the issues themselves.[161] The language of litigation can thus

---

for instance, demonstrated how legal process in America tends to get funneled into *judicial* process, creating a "method of policymaking" focused on "rights, duties, and procedural requirements" rather than cooperation, cost-efficiency, or efficacy. ROBERT A. KAGAN, ADVERSARIAL LEGALISM: THE AMERICAN WAY OF LAW 9 (2001). Kagan documents this tendency in the regulatory, as well as in the criminal and civil context, and concludes that the centrality of judicial process to American policy and dispute resolution creates a system in which outcomes are less predictable, but resolutions more costly, than in comparable advanced democracies. *Id.* at 3-4. Problems are also more likely to be resolved through litigation in the first place; judges are more influenced by personal politics; lawyers play a larger part in shaping legal outcomes even when those outcomes affect more than just their clients; legal change depends more on the pursuit of interests by organized groups; and penalties for loss are stiffer. *Id.* at 3. In the regulatory context, this leads to a nitpicky and adversarial regulatory style that tends to prescribe precise methods and actions rather than overall goals and in which regulators and regulated parties are pitted against one another, often in court, rather than aiming for cooperative relationships. *See id.* at 191. Kagan finds that this regulatory style is both more expensive and less effective than the more goal-oriented, cooperative style of comparable nations. *Id.* at 3-4, 191-92. He also suggests that this trend has been with us for some time, quoting Tocqueville's comment that "[s]carcely any political question arises in the United States that is not resolved . . . into a judicial question." *Id.* at vii (quoting ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 290 (Vintage Books 1945) (1835)) (internal quotation marks omitted); s*ee also* Thomas W. Merrill, *Article III, Agency Adjudication, and the Origins of the Appellate Review Model of Administrative Law*, 111 COLUM. L. REV. 939, 939-46, 997-1000 (2011) (suggesting that American-style judicial review of administrative action, in which courts not only determine whether an agency acted within its authority but also adjudicate what are effectively policy judgments, may lead to a somewhat chaotic jurisprudence based in policy preference and a continuing incorporation of time-bound administrative trends in place of technocratic expertise or executive policy decisions).

161. *See, e.g.*, JERRY L. MASHAW, BUREAUCRATIC JUSTICE: MANAGING SOCIAL SECURITY DISABILITY CLAIMS 15 (1983) (showing that even administrative action that has direct effects on individuals and their rights functions primarily via an "internal law of administration" that precedes, and is largely invisible to, judicial review). As Mashaw demonstrates, focusing on judicial review of administrative action largely misses the point: because the ongoing work of administration happens not in courts but in administrative agencies, court appearances mark only the exceptional moments when administration is pulled out of the agency. *See* JERRY L. MASHAW, CREATING THE ADMINISTRATIVE

unproductively constrain analysis, directing it away from broader questions of accountability in a representative democracy.[162]

The litigation-oriented search for a discrete act that violates a particular right or imposes a particular harm does not capture the power of predictive database use.[163] Neither does the framework of privacy, which focuses on the individual's ability to keep independently extant information from circulation or to cordon off certain areas of conduct from government control.[164] It is not that rights are not at stake; it is just that more is at stake than rights.

V. TOWARD AN EFFECTIVE LEGAL REGIME

Existing laws controlling terrorist watch lists focus on factual accuracy and individual rights, not on predictive

---

CONSTITUTION: THE LOST ONE HUNDRED YEARS OF AMERICAN ADMINISTRATIVE LAW 302-06 (2012). Relatedly, William Chase has traced the long-time academic focus on courts in administrative law to the structure of legal education, which, "intensely committed to the study and teaching of the work product of the traditional courts," framed the study of administration as a study of what courts thought about administration. WILLIAM C. CHASE, THE AMERICAN LAW SCHOOL AND THE RISE OF ADMINISTRATIVE GOVERNMENT 20 (1982).

162. Richard Thompson Ford has also criticized the court-centered approach of American law, scholarship, and politics from a different but related perspective, arguing that this approach degrades the goals of social movements by shifting attention from structural impediments to equality and other social problems, instead keeping people focused on the narrower, and malleable, question of individual rights. *See, e.g.*, RICHARD THOMPSON FORD, RIGHTS GONE WRONG: HOW LAW CORRUPTS THE STRUGGLE FOR EQUALITY 21 (2011) ("[R]ights cannot change deep-seated institutional and cultural injustices without changing the institutions and culture in which they are rooted.").

163. For a discussion of ways in which arbitrary classification may infringe on rights other than privacy, see Aaron H. Caplan, *Nonattainder as a Liberty Interest*, 2010 WIS. L. REV. 1203, 1203 (2010) (arguing that "the rule against singling out persons for punishment without trial" which constitutes the Constitutional ban on bills of attainder "should be recognized as a due process liberty interest" to render improper inclusion on a government blacklist actionable).

164. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1162-63 (2004) (describing American notions of privacy as focused on limiting state control over certain areas of life, while European notions focus on limiting the distribution of information about individuals more generally).

process and broad effects. The distinctive power of these databases to shape political policy and social imaginaries therefore remains largely unregulated and unacknowledged. When we look beyond individual rights and ask about the government's responsibilities to the society it shapes, however, it is this distinctive power that calls out for constraint.

Creating those constraints is no easy task for three primary reasons. First, there is no precise science to predicting human conduct. It is difficult to require governments to use reliable predictive methods when we do not know which methods are reliable. Second, the social effects of watch lists emerge gradually and are not easily tracked. It is difficult to require governments to minimize or control a watch list's social effects when we do not know how, or how much, it will affect society. Third, watch lists are subject to complex pressures. We want them to be correct in their predictions, but not so all-knowing that they create social classes. We want them to be complete, but not to skew our perceptions of the conduct they address or allow arbitrary classifications. And we want them to be cost-justified, but do not always know how to measure their costs and benefits. It is difficult to require governments to change their practices when we want the changes to have multiple, possibly incongruent, effects.

At the same time, such difficulties are not new to agencies that regulate conduct. Limits on knowledge, resources, and authority make devising effective regulations difficult. Competing interests complicate regulatory goals. Yet agencies still act in the face of these difficulties. Creating an effective legal regime to constrain watch lists entails applying to the government the very kind of goal-oriented mandates, based on partial knowledge, that government agencies often apply to those they regulate. It means implementing an "internal law of administration" that resembles in crucial respects external administrative regulations.[165]

---

165. *Cf.* Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. 575 (2010). Rascoff argues that the traditional analogy of domestic intelligence to criminal law enforcement has led to a "governance vacuum," *id.* at 582, because the analogy belies the actual work of intelligence. *Id*. at 581-82. Intelligence work, Rascoff argues, is essentially a kind of "risk assessment," a crucial underlying feature of regulation. *Id.* at 582. Intelligence work is, therefore,

As I discuss above, research on institutional knowledge production suggests that the more institutions buy into their own claims to possess full, objective knowledge about a given object, the more likely they are to fail to notice aspects of the object that exceed their grasp. This suggests, perhaps paradoxically, that accountable prediction requires a good dose of self-doubt. This Part proposes ways to build self-doubt into watch lists.

A. *Feedback, Internal Consistency, Updating, Acknowledged Subjectivity*

Agencies should be required to create *feedback* mechanisms that allow for continual assessments of the extent to which watch list predictions prove correct. Agencies should use those feedback inquiries to determine whether a watch list is *internally consistent*, in the sense that it actually targets the kind of activity it is meant to address. When there is inaccuracy or inconsistency, agencies should *update* their watch list processes and predictions accordingly. I also suggest that agencies should explicitly *acknowledge the subjectivity* inherent in watch list judgment, illuminating rather than obscuring the moments at which evaluative judgment comes into play.

My proposals ask agencies to assess both the quality of their watch lists and the process by which they are produced. And they require agencies to act on those assessments. Currently, watch list costs are presumed to be negligible. That assumption relieves agencies of assessing their benefits. Once we acknowledge that watch lists exact costs even beyond their monetary upkeep, it is clear that they require assessment and improvement.

To implement feedback and updating, watch lists should be structured with the assumption that both predictions and predictive processes will require amendment. Individual listings should be subject to revision, of course: new information should affect old decisions. But so should predictive criteria and the theory

---

amenable to the full array of regulatory governance tools. *See id; see also* Jerry L. Mashaw, *Reluctant Nationalists: Federal Administration and Administrative Law in the Republican Era 1801–1829*, 116 YALE L.J. 1636, 1739 (2007) (discussing the "internal law of administration" as a system of administrative self-constraint).

that connects them to the relevant conduct: the system should have provisions not only for altering individual predictions, but also for changing how agents make predictions in the first place.[166]

At present, watch lists lack such provisions. Instead, they reflect confidence that the assumptions guiding them will hold true and that their predictions will be correct. Instead of regular self-assessments built into the evaluative process, they are often subject only to partial or periodic external reviews, such as the occasional studies carried out by inspectors general or the Government Accountability Office.[167] Each such review has its own focus, objectives, and methods, leading to evaluations that, though often excellent, are still piecemeal.[168]

Commentators have pressed for administrative agencies to be subject to more frequent, more regular, and more searching evaluations. Mariano-Florentino Cuéllar, for instance, has proposed creating an independent commission to audit discretionary agency actions.[169] Cuéllar suggests evaluating random samples of discretionary decisions to see how well they adhere to decision-making standards articulated prior to the review.[170] In contrast to judicial review, which casts only a limited light on a very few agency actions, in-depth audits would give legislatures, the public,

166. The consolidated terrorist identity watch list operated by the National Counterterrorism Center (NCTC) does have mechanisms for removing individuals from the watch list, though these are in practice often not implemented. THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES, *supra* note 53, at xvi (finding, in a sample of eighty-five closed investigations, that seventeen entries correctly remained on the watch list for other reasons or were properly removed in a timely manner; sixty-one entries were properly removed but not in a timely manner; and seven entries improperly remained on the list). What is required, though, is not only a way to adjust individual listings but a way to change systemic criteria for listing.

167. *See* Mariano-Florentino Cuéllar, *Auditing Executive Discretion*, 82 NOTRE DAME L. REV. 227, 291 (2006) (discussing the limitations of current executive review mechanisms).

168. *Id.*

169. *Id. at* 231-32.

170. *Id.* at 240.

and agencies themselves a better understanding of everyday administrative activities.[171]

Relatedly, Michael Greenstone has proposed creating a new legislative office to evaluate the actual impact of regulations over time.[172] He also suggests establishing a standard, agency-internal "retrospective analysis" of the actual effects, including the actual costs and benefits, of regulations.[173] These proposals aim to overcome the unrealistic optimism endemic to American administration, which historically has estimated the "*likely* benefits and costs" of regulations "*before* they are enacted."[174] "[B]ecause the regulations are untested" prior to their enactment, however, it is impossible to assess their actual effects.[175] This administrative attitude thus has things a bit backward, as "[o]nce a regulation is implemented, it goes on the books and generally stays there unexamined for years and in some cases decades,"[176] even if its costs or benefits differ from those predicted.

Cuéllar and Greenstone suggest that regular assessments of government actions can help overcome the unrealistic impulses of decision makers by confronting them with the actual results of their decisions.[177] Watch lists

---

171. *See id.* at 252-274.

172. *Improving Regulatory Performance: Lessons from the United Kingdom: Statement Presented to the S. Budget Comm. Task Force on Gov't Performance* 4 (2011) (statement of Michael Greenstone) [hereinafter *Improving Regulatory Performance: Lessons from the United Kingdom*], *available at* budget.senate.gov/democratic/index.cfm/files/serve?File_id=b1b6d27f-8f1c-4370-a42e-432ebf4d8885 (proposing a new office, modeled on the Congressional Budget Office and housed within Congress, to evaluate the effects of implemented regulations); *see also* Exec. Order No. 13563, 76 Fed. Reg., 3822 (Jan. 18, 2011), *available at* www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf (requiring agencies to "consider how best to promote retrospective analysis of rules that may be outmoded, ineffective, insufficient, or excessively burdensome, and to modify, streamline, expand, or repeal them in accordance with what has been learned").

173. Exec. Order No. 13563, 76 Fed. Reg. at 3822.

174. *Improving Regulatory Performance: Lessons from the United Kingdom*, *supra* note 172, at 3.

175. *Id.*

176. *Id.*

177. Other scholarship suggests that similar reviews can benefit intra-governmental practices as well. *See* Shapiro & Morrall III, *supra* note 29, at 190

inherit the unrealistic optimism and confidence of the bodies that create them. That self-confidence encourages the ossification of evaluative approaches to a dynamic object; it also encourages some sloppiness in applying the evaluative approaches.[178] Building in updating mechanisms could check these unrealistic impulses by incorporating evolving understandings of the phenomena that databases address. And it would allow databases to keep up with the changing nature of these phenomena—facts on the ground—which themselves react and change in response to government actions.[179]

Building in feedback and updating mechanisms would also help alert government bodies to mismatches between the criteria used to make predictions and the kind of prediction being made.[180] That kind of mismatch is evident

---

(finding that increasing information used for benefit-cost analysis did not increase the benefits of regulations, and that political salience decreased them).

178. THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES, *supra* note 53, at v, vi, 1 (finding the process for listing individuals who are not currently under investigation by the FBI on FBI terrorist watch lists flawed: the agency routinely failed to follow its own policy for reviewing proposals to include new names on the watch lists; had "no formal or active process to update or remove" names that had not been reviewed; and commonly included names with "little or no information explaining why the subject may have a nexus to terrorism"; the agency had no way to remove or modify entries submitted via particular routes; and 35% of the over 68,000 identities originating from FBI watch lists were "associated with FBI cases that did not contain current . . . terrorism designations," but rather arose from cases that had been closed or were "unrelated to terrorism").

179. *See, e.g.*, HACKING, THE TAMING OF CHANCE, *supra* note 81, at 2 (noting that descriptions of and theories about human conduct tend to have a "feedback effect" that affects the very conduct they address). Hacking focuses on social-scientific descriptions and theories, but the point applies with equal force to government-based understandings of human conduct, which are themselves often based on social-scientific theories and their popularizations, as well as prevalent social attitudes more generally. Perhaps most crucially, government-based understandings can act on the world in even more powerful ways than social-scientific theories, for instance by subjecting classes of people to legal requirements or increased attention from government agents.

180. *Cf.* HARCOURT, *supra* note 33, at 23. Harcourt argues that the goal of profiling—to catch criminal acts within a particular population—can be counterproductive to achieving the broader goal of law enforcement—to reduce crime in general—because the profiled population may reduce its criminal behavior less than the non-profiled population may increase its own criminal behavior. *See id.* In other words, Harcourt argues, even though profiling is used

in the FBI's VGTOF list, which connects gang-based criteria to terrorist conduct.[181]

Several factors can help indicate how attenuated predictive criteria are from the conduct predicted *ex ante*. We can ask how *precise* the criteria are. Do they pick out specific facts that are easily distinguished from other facts, or are they fairly mushy? We can ask how *standard* the criteria are. Do they compel a particular prediction across evaluators, or do they leave a lot of room for individual interpretation? And we can ask how well *articulated* the theory underlying the criteria is. Is there a strong argument that the criteria actually identify the conduct the database addresses?

Most importantly, however, the relation of criteria to prediction is open to empirical testing ex post.[182] Feedback and updating mechanisms should compel those who maintain predictive government databases to evaluate whether the information they use actually serves, over time, to pick out the conduct they target.

For example, the National Security Entry-Exit Registration System (NSEERS), which required people from certain countries to register with DHS upon arrival in the United States and at regular intervals thereafter, was meant to address national security threats.[183] Based on an implicit prediction that visitors from particular countries would pose heightened national security threats, this database contained information about the identities and location of immigrants and visitors from twenty-five countries.[184] But the extent to which simply having that information effectively targeted national security risks was

---

as a tool of law enforcement, the effects of profiling turn out to be inconsistent with the goals of law enforcement. *See id.*

181. *See* discussion *supra* Part I.B.

182. *See* discussion *supra* Part V.A.

183. The countries whose residents were required to register were: "Afghanistan, Algeria, Bahrain, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, North Korea, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen." Removing Designated Countries From the National Security Entry-Exit Registration System (NSEERS), 76 Fed. Reg. 23,830 (Apr. 28, 2011) [hereinafter Removing Designated Countries From NSEERS].

184. *See id.*

low: a review of publicly available information about the program found it "unsuccessful as a counterterrorism tool."[185] Its main effect was to net ordinary people who had overstayed their visas or failed to comply with the somewhat arcane NSEERS requirements themselves.[186]

It seems likely that DHS evaluated the actual results of NSEERS and noted the internal inconsistency of information with target, because the NSEERS program was suspended in 2011 in order to "eliminate redundancies; streamline the collection of data for individuals entering or exiting the United States, regardless of nationality; and enhance the capabilities of our security personnel."[187]

The more the criteria used to make a watch list prediction are attenuated from the conduct predicted, then, the more we can expect a watch list to miss its purpose of predicting specific conduct on the part of particular people.[188] Requiring databases to include provisions for feedback-based revision may help counteract such inconsistencies.

Finally, one implication of studies like James Scott's is that a watch list built on an assumption that its standards are objective and its knowledge totalizing will inevitably confuse the priorities of its creators with the realities of its objects.[189] Similarly, when the subjective elements of prediction are obscured, those making and using databases may easily mistake opinion for fact. To counteract these

---

185. PENN STATE UNIV., DICKINSON SCHOOL OF LAW, NSEERS: THE CONSEQUENCES OF AMERICA'S EFFORTS TO SECURE ITS BORDERS, 6 (Mar. 31, 2009), www.adc.org/PDF/nseerspaper.pdf.

186. *See id.*

187. *Important NSEERS Information*, IMMIGRATION DAILY (May 20, 2011), http://www.ilw.com/immigrationdaily/news/2011,0524-nseers.shtm; *see* Removing Designated Countries From NSEERS, *supra* note 183, at 23,831. DHS has not technically cancelled NSEERS but only suspended it by relieving any visitors from its reporting requirements. The regulations creating the program are still in effect, and the program thus stands ready to be re-implemented at any time.

188. *Cf.* David Zaring & Elena Baylis, *Sending the Bureaucracy to War*, 92 IOWA L. REV. 1359, 1364 (2007) (arguing that bureaucracies created for limited civilian purposes will predictably fail when pressed into national security service because of a mismatch of goals and techniques).

189. *See* discussion *supra* Part III.B.

results, an effective legal regime for predictive government databases should require that watch lists acknowledge the subjective and partial nature of their predictions and, if possible, use them to the watch lists' advantage by encouraging better judgment in government agents.

Instead, watch lists are often structured to obscure their dependence on judgment, phrasing their evaluative process in objective terms—as though the mere existence of information itself necessitated certain predictions. This misrepresents the actual evaluative process of prediction, which requires that information be interpreted.

Agents and agencies facing outside audiences may naturally be tempted to present watch listing processes as more objective than they really are. But such representations may also obscure the role of subjective judgment to internal audiences: the very agents making the predictions. Agents exercising their subjective judgment may be encouraged to think of their activity as merely reading truth off of information. Such misunderstandings exacerbate the self-blinding effects of overconfidence.

Acknowledging subjective components, in contrast, can increase users' awareness of the limitations and quirks of database predictions. Combined with external feedback, it can also help governments harness subjectivity by focusing training or changing criteria based on the database's real-world performance.

B. *Directions for Reform*

How can we include feedback, updating, internal consistency, and acknowledged subjectivity in watch lists to counteract their perverse incentives? The clearest route would be statutory: Congress should amend the Privacy Act to eliminate or tighten the exemptions to its relevance, timeliness, completeness, and accuracy requirements.[190] This would affect many databases, not just watch lists. But the effect would be salutary. In areas where certainty is relatively easy to achieve—either because the database merely compiles independently existing information or because its predictions are well-tested and based on a

190. 5 U.S.C. § 552a(e)(5) (2006).

wealth of historical data—the requirements should be relatively simple to fulfill.

In areas of high *un*certainty like terrorist watch lists, in contrast, imposing these requirements would push agencies to consider what relevance, timeliness, completeness, and accuracy means in a particular context. The agency could define these statutory terms in regulations specific to each particular watch list, which would require it to determine what level of relevance, timeliness, completeness, and accuracy was appropriate for that watch list. This process would encourage agencies to gather evidence about how watch list predictions fare in the real world in order to determine what the statutory terms should mean in any given context.

The agency's definition of these statutory terms should appear in the System of Records Notice the Privacy Act already requires when a database is created or modified.[191] This would require the agency to consider the purpose of its predictions and think about how they relate to their real-world objects.[192] It would provide pre-articulated standards that would render the database amenable to external or internal audits.[193] And it would increase the transparency of watch lists, allowing executive actors, legislators, and the public to evaluate them.

For instance, an early articulation of how the VGTOF's criteria were meant to pinpoint terrorist activity might have alerted the agency to the potential mismatch of some criteria to the database's target. If such an articulation would reveal sensitive information, the modified Privacy Act provision could contain a secrecy clause allowing agencies to make the articulation internally, or to Congressional bodies only.[194] While a public enunciation of standards facilitates widespread evaluation of the social effects of a watch list, the main thrust of my proposal is that

---

191. § 552a(e)(4).

192. Such standards might resemble the data "minimization" efforts that the Foreign Intelligence Surveillance Act (FISA) requires before information may be shared. *See* 150 U.S.C. § 1801(h) (2006).

193. *See* Cuéllar, *supra* note 167, at 285-86.

194. *Cf.* David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 334-35 (2010) (proposing that government secrets should be revealed to different publics depending on their level of sensitivity).

explicit articulation—even to limited audiences—should be part of the process of developing such databases.

Once a watch list is developed, moreover, agencies should be required to subject it to regular investigation to determine how it actually functions. A Privacy Act amendment should require agencies to develop ongoing evaluations of how watch list predictions hold up. The outlines of the assessment protocol should be provided in the System of Records Notice, which should explain how the agency plans to review the watch list's efficacy and how often it plans to implement reviews.

These evaluations should be tied to ongoing revisions of predictions and predictive processes, so that updating is a natural and continuous result of feedback. Self-assessments, in other words, should be followed by improvements based upon them. The same Privacy Act amendment should require agencies to update their System of Records Notice for each watch list periodically to explain, in general terms, what self-assessment has revealed and what the agency will do about it. Such a process would make watch lists more efficacious and more transparent. It would also serve as a signal to agents and agencies that watch list judgments are imperfect and subject to modification. A fuller report distributed to relevant agency personnel should detail watch list failings, which would also help keep agents aware of the quality of their predictions.

The agency's feedback and updating approach, furthermore, should itself be subject to external reviews. These investigations could take a variety of forms. They may involve in-depth audits of database predictions like those suggested by Cuéllar for other discretionary practices.[195] They may also, on the model of scientific studies, include long-term studies of specific watch-listed subjects to determine the extent to which predictions or investigative actions based on these evaluations turn out to be reliable.[196]

---

195. *See* Cuéllar*, supra* note 167, at 232, 252-74.

196. This resembles the retrospective review of actual policy effects suggested by Greenstone in *Improving Regulatory Performance: Lessons from the United Kingdom*, *supra* note 172, at 3, and initiated by Exec. Order No. 13563, 76 Fed. Reg. at 3822, at 3822.

A Privacy Act amendment is the best way to impose these new constraints. But an agency concerned with the efficacy of its watch list could implement these proposals on its own. Although a change in incentive structure might work best when imposed by the legislature, an agency leadership dedicated to efficacy can implement such change from the inside.

Another agency-internal change that would improve watch list judgments would remind evaluators of the subjective nature of their evaluations. Such efforts might include reverting to more narrative, explanatory approaches that require agents not only to provide information supporting their predictions but also to make explicit their own interpretations of that information. This approach would counteract the implications of objectivity that checklists of criteria create.

Narrative explanations should be included in ongoing reviews to help determine how government agents actually make predictions about terrorist conduct. They could also be subjected to dialogue and dissent by having several agents participate in making a prediction.[197] This would increase attention to reasoning and evaluative processes and awareness of personal predilections.

Of course, these are not simple fixes, and they are not guaranteed to work. Promoting dialogue may exacerbate patterns of weak reasoning or encourage groupthink or reasoning to extremes. At the same time, this approach might at least remind agents that evaluation, rather than merely information collection, is the central step in watch list predictions.

These may seem like costly measures to take simply to manage a list. Watch lists, after all, are not generally seen to be a method of implementing or creating policy. They are merely a tool for keeping track of those that policy addresses. But this view accepts the seemingly neutral, objective nature of databases. If databases are mere repositories of information available for other uses, there seems little point in expending effort to control them.

---

197. Such a dialogic endeavor resembles so-called red team analysis or "[d]issent [c]hannel" provisions that aim to encourage productive internal disagreements. *See* Katyal, *supra* note 10, at 2328.

But if we see watch lists as themselves creating knowledge through the evaluation of individuals, the question of costs looks different. The classification of individuals in watch lists can have profound implications for how they can live their lives. And the facts that watch lists report about our world can influence our policies: how much effort we want to spend on combating terrorism and what kind of effort we think will work. In this way, watch lists become black boxes undergirding larger theories, policies, and worldviews.[198] They tell us what our social world looks like: who inhabits it and what dangers it poses. And we use what they tell us without knowing how they came to their conclusions or how valid those conclusions are. In this light, it becomes more important to assess how much the facts that watch lists produce correspond with reality.

CONCLUSION

A. *Other Predictive Databases*

This Article has focused on terrorist watch lists. But terrorist watch lists are just one example of a type: government databases used to predict human conduct. Such databases will be subject to radically different incentive structures than those surrounding terrorist watch lists. For instance, correct predictions in some databases have a clear monetary payoff and operate in relatively low-salience fields. When that is the case, we can expect agencies to incorporate self-assessment mechanisms naturally into their predictive processes. Self-assessment is relatively easy when money is at stake both because the accuracy of a prediction is presented in clear terms and because monetary value makes the relationship between false negatives and false positives easier to quantify. And lower salience puts less pressure on agencies to appear active, allowing for simpler ways to implement corrections that improve efficacy.

198. *Cf.* LATOUR, *supra* note 66, at 130-31 (arguing that scientific citation itself, quite aside from experimental proof, has a fact-making power, because repeated citation of a claim based on an experiment tends to give the claim an unquestionable factual status in the community of scientists, rendering the original evidence and analysis on which the claim was based a "black box" impervious to further investigation).

But in similarly high-salience fields with no clear way of quantifying accuracy, we can expect databases used for prediction to face similar problems as terrorist watch lists. This is so irrespective of whether the databases are created and managed by administrative agencies, as terrorist watch lists are, or by Congress itself. For instance, Congress has required all states to keep publicly accessible registries of convicted sex offenders.[199] The government itself does not offer a prediction in this case. It only mandates the disclosure of information so that individual members of the public may make their own predictions about the convict's future conduct.[200] At the same time, that mandate also implies that this is the information the public needs to form a reliable assessment: the concept of an offender registry is based on the implicit prediction that people convicted of certain crimes are likely to recidivate.

Yet empirical research has repeatedly called into question the predictive utility of previous sex offenses for recidivism.[201] And neither the statute nor its implementing

---

199. *See generally* Adam Walsh Child Protection and Safety Act of 2006, Pub. L. 109-248, 120 Stat 587, 596 (2006) (codified as 42 U.S.C. § 16912 (2006).

200. *See id.* This is a form of "mandated disclosure." *See* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 649 (2011). Ben-Shahar and Schneider explain that "[t]he technique requires 'the discloser' to give 'the disclosee' information which the disclosee may use to make better decisions and to keep the discloser from abusing its superior position." *Id*. The aim is "to improve decisions people make in their economic and social relationships and particularly to protect the naive from the sophisticated." *Id.* Ben-Shahar and Schneider document the failure of mandated disclosure to achieve these goals and present a number of reasons for that failure. *See id.* at 679 (beginning discussion of reasons for failure). One benefit of subjecting registries to the self-assessment mechanisms I propose discussion *supra* Part V.B., is in revealing which registries fail to achieve their goals and why.

201. *See, e.g.*, HUMAN RIGHTS WATCH, NO EASY ANSWERS: SEX OFFENDER LAWS IN THE US, 3, 9 (Sept. 2007), http://www.hrw.org/sites/default/files/reports/us0907webwcover.pdf (documenting the absence of "convincing evidence of public safety gains" from registration requirements and noting that such requirements may be "counterproductive" because "the proliferation of people required to register" for non-serious crimes "makes it harder for law enforcement to determine which [registrants] warrant careful monitoring"). Registration also diverts law enforcement resources to tracking registrants, determining who has failed to register, and prosecuting those who do so, even though these expenditures do little to effectuate the database's goal of lowering the incidence of and opportunity for sex crime commission. *See, e.g.*, Andrew J.

regulations articulate a theory of recidivism to explain the registration requirements. It may well be that registration prevents recidivism. But it may also be that severe registration requirements inspire greater efforts to avoid registration and divert law enforcement attention from sex offense to registration maintenance. Without articulating how the requirements relate to the law's goals, it is difficult for the government to assess the system's internal consistency and efficacy.[202]

The Sex Offender Registration and Notification Act ("SORNA"), which is the sex offender registration statute, does leave an avenue open for self-assessment: it requires the Attorney General to constitute a task force to study the relative merits of individualized risk assessments versus registration based on conviction category.[203] However, the

---

Harris and Christopher Lobanov-Rostovsky, *Implementing the Adam Walsh Act's Sex Offender Registration and Notification Provisions: A Survey of the States*, 21 CRIM. JUST. POL'Y REV. 202, 203 (2010) (noting that no state had achieved compliance with the statute's registration requirements by the deadline of July 2009); Wayne A. Logan, *The Adam Walsh Act and the Failed Promise of Administrative Federalism*, 78 GEO. WASH L. REV. 993, 1009 n.96 (2010) (noting the high costs of implementing the statute's registration and notification requirements and quoting the California Sex Offender Management Board as stating that this cost would exceed the amount of federal funding that California would forego if it failed to implement the statute's provisions).

202. For instance, noting that "SORNA's tiering structure" does not "supersede[]" but supplements local "jurisdictions' existing risk assessment processes" for sex offenders, the DOJ has called the notion that the tiering structure "is meant to help predict sexual reoffense" a "misconception." DEP'T OF JUSTICE, OFFICE OF SEX OFFENDER SENTENCING, MONITORING, APPREHENDING, REGISTERING, AND TRACKING, SMARTWATCH, SORNA: ADDRESSING THE CHALLENGES (2009), *available at* http://www.ojp.usdoj.gov/smart/smartwatch/09_august/SORNA_challenges.html ; *see* 42 U.S.C. § 16911 (2006) (defining the sec offender tiers). But it is unclear what purpose other than prediction the system could serve, and the DOJ instructions do not suggest any. The statute itself states that it was passed "[i]n order to protect the public from sex offenders and offenders against children," which suggests that tiers are allocated based on the likelihood of offense. 42 U.S.C. § 16901 (2006). This mismatch between the official explanation of the statute and the statute's only apparent purpose makes it yet more difficult to assess the database's effects.

203. Adam Walsh Child Protection and Safety Act of 2006 § 637, 120 Stat. at 645-46. The statute requires the Attorney General to present the task force's conclusions to Congress within 18 months of SORNA's passage, but a search of the Department of Justice website produced no such study.

statute contains no provisions for updating or evaluation of the extent to which the registry serves its goals at all.

None of these defects should be surprising given the analysis in this article. Sex offenses, like terrorism, are a complex, high-salience area with a limited amount of historical data on which to base predictions and no clear monetary payoff for correct predictions. We should expect government databases in this arena to be internally inconsistent, to contain few self-assessment mechanisms, to rely on implicit assumptions rather than articulated theories, and to appear more objective than they really are. While my proposals would work differently in the legislative arena of SORNA—where Congress would have to impose limits not just on agencies, but on itself—the substance and logic carry over. As government databases continue growing, moreover, and as their uses continue to expand, we can expect ever more databases to be used for prediction, and ever more to suffer from the problems I have described.

B. *Dilemmas of Knowledge*

This Article has drawn attention to the distinctive features of terrorist watch lists and other databases used to predict human conduct. I have argued that characteristics such as ease of combination, portability, decontextualization, impersonality, and diffusion of evaluative labor can make such databases powerful. But these same characteristics can also undermine them, causing problems for the agencies that maintain them, the governments that commission them, and the public they serve.

Despite this potential for harm, the legal regime that constrains government databases recognizes only the harms they cause individuals, such as producing inaccurate records, invading privacy, and, at the margins, infringing a right to travel. I have proposed addressing that legal lacuna by requiring such databases to build in efficacy standards; to test and revise their prediction protocols; and to make their subjective elements explicit to those who use them.

My analysis raises two related conundrums. First, the conundrum of overconfidence and self-correction. I conclude above that states trust their conclusions at their peril, and that attempts at ultimate, total knowledge will predictably fail. I propose a way to guard against this failure: give up attempts at total knowledge; assume that any prediction

will be partial and have flaws; construct databases with ongoing self-correction mechanisms to account for inevitable failures.

But the solution seems to ignore the problem. Doesn't this attempt at self-correction display the very self-aggrandizing overconfidence it is meant to combat? Can we avoid overconfidence in results by substituting overconfidence in methods?

There is no satisfying way out of this contradiction, which pits our increasing knowledge of the world against our increasing understanding that knowledge is always limited. The real answer to the conundrum would be to eliminate predictive government databases altogether. But we have known for decades that modern states are defined by their production of knowledge about their populations. The portable, combinable, diffuse nature of predictive government database use is, in turn, characteristic of modern forms of knowledge more generally. Calling for the elimination of such databases altogether would be asking the scorpion not to sting the frog. My proposals are thus not solutions to the underlying problem, but ways to soften its worst symptoms.

Second, I state above that the broader normative issues that these databases raise have to do with how people conceptualize their society. Governmental predictions create social categories that affect social structure and political policy. But the reforms I propose do not stop governments from making predictions or having social effects. Doesn't insisting on better categories miss the point?

Again, there is no ultimate solution: government representations will always affect, and not just reflect, the societies they represent. Again, all we can strive for is amelioration. The first step is recognition: the effects of government pronouncements go deeper when they are not recognized as effects at all. Requiring watch lists to confront their users with the complexities of their internal production and with the vagaries of the world they analyze brings their contingencies to the fore. That will not be the last word on the issue of their social effects. But it would allow us to start a conversation about them.

Government databases used for predictions about human conduct are currently treated as neutral instruments of government policy. Bringing their limitations and effects to the surface refigures them as

creative creatures that can affect policy as well. That provides a first step toward dealing with their normative implications. Both the dilemma of knowledge and the inevitability of effects admit of only partial solutions; but partial solutions are better than none at all.