UIC John Marshall Journal of Information Technology & Privacy Law

Volume 27
Issue 2 *Journal of Computer & Information Law - Winter 2009*

Article 3

Winter 2009

Extending the Exclusionary Rule: Enforcing Data Quality in National Security Databases and Watch Lists, 27 J. Marshall J. Computer & Info. L. 257 (2009)

Christine M. Whalley

Follow this and additional works at: https://repository.law.uic.edu/jitpl

 Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Christine M. Whalley, Extending the Exclusionary Rule: Enforcing Data Quality in National Security Databases and Watch Lists, 27 J. Marshall J. Computer & Info. L. 257 (2009)

https://repository.law.uic.edu/jitpl/vol27/iss2/3

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

EXTENDING THE EXCLUSIONARY RULE: ENFORCING DATA QUALITY IN NATIONAL SECURITY DATABASES AND WATCH LISTS

CHRISTINE M. WHALLEY*

Since its inception, the exclusionary rule has been aimed at deterring misconduct by police officers and law enforcement agents. It is widely believed to deter deliberate, reckless, grossly, or systemic negligent conduct by law enforcement agents. Increased reliance by law enforcement agencies and their agents on expansive, interconnected information suggests that the exclusionary rule needs to be expanded beyond just the acts of the officers and agents and be applied to the agency itself, where there is evidence that poor data quality standards produced the reckless or negligent conduct. When so much of our liberty rests on the quality of the data in these databases and watch lists, it is irresponsible to allow such systems to be exempt from legislatively mandated data quality standards. The government must endure the sanction imposed upon it under the exclusionary rule – for it is a constraint on the power of the government, not just some of its agents, to preserve the fundamental protection under the Fourth Amendment to be secure in our persons, homes, papers, and effects. This article explores the current framework within which data quality of criminal records and national security watch lists are maintained and how extending the exclusionary rule to the underlying systems of information on which the law enforcement agencies and their agents so heavily rely can increase the data quality of these systems.

* Juris Doctorate (2010), Pace University School of Law, with more than 20 years of experience in Information Security. I may be contacted at *christine@whalley.org*. I gratefully acknowledge the patience and support of Ian Whalley, when it appeared the law library was my new home and I finished this article during our holiday in the Orkney Islands. I also gratefully acknowledge the encouragement and support from Mark R. Shulman, Marie Stefanini Newman, and Bridget J. Crawford as I undertook this endeavor. In addition, I appreciate the assistance from the entire editorial team at the Journal of Computer and Information Law.

I. INTRODUCTION

What happens when you are about to embark on a business trip only to discover that you are listed on the "No Fly List" and are unable to board your flight?[1] What do you do when you are stopped for a traffic violation and suddenly find yourself being arrested because the police officer has received information that there is an outstanding warrant for you?[2] What do you do when you find that you are being whisked away to a foreign country for interrogation because you are incorrectly suspected of being a terrorist?[3]

Too often the knowledge of such erroneous information only comes when one is at the wrong end of the situation and one's liberty, reputation, person, house, papers, or effects have been violated. In the situations described above, would the average person know what actions to take to have the information corrected, who should be responsible for making the corrections, and how to ensure that the corrections were indeed made in a timely fashion? Particularly, after September 11, 2001, there has been a concerted effort by the government and various agencies within the United States government to create an "information sharing environment"[4] that accumulates data on persons and entities. This data then provides the basis for terrorist watch lists, no-fly lists, criminal records, and other data that is used by law enforcement and various agencies in support of national security.

The government has faced increasing pressure to improve its collection and use of information in order to be more vigilant against terrorists and their activities. The lack of information and the government's failure to share such information was cited as the "single greatest failure of our government"[5] leading up to the 2001 attacks on the United States. While accumulating and sharing this information may provide protection to our nation, it is vital that the government also ensure the quality of the cascading information it shares in order to preserve our fundamental protections under the Constitution to be secure against unreasonable

---

1. Story regarding a colleague of the author who discovered that a variation of his name was on the "No Fly List" maintained by the Transportation Security Agency. *See also* Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, ASSOCIATED PRESS, Sept. 29, 2004; Joe Sharkey, *Not too Small to Appear on a Big No-Fly List*, N.Y. TIMES, Sept. 29, 2008, *available at* http://www.nytimes.com/2008/09/30/business/30road.html?_r=2&oref=slogin.

2. *See* Arizona v. Evans, 514 U.S. 1 (1995).

3. *See* Arar v. Ashcroft, 532 F.3d 157 (2d. Cir. 2008).

4. Exec. Order No. 13,388, 70 Fed. Reg. 62023 (Oct. 25, 2005).

5. *Federal Support for Homeland Security Information Sharing: Role of Information Sharing Program Manager: Hearing before the Subcomm. on Intelligence Information Sharing and Risk Assessment of the House Comm. on Homeland Security*, 109th Cong. 23 (2005) (statement by Lee Hamilton, Vice Chairman, 9/11 Public Discourse Project).

searches and seizures of our persons, houses, papers, and effects[6] and to not be deprived of our life, liberty, or property without due process.[7] In the 2009 decision *Herring v. United States*, Chief Justice Roberts writing for the majority held that the good faith exception to the exclusionary rule even applied to situations where negligent police recordkeeping resulted in an unreasonable search and seizure.[8] This exception to the exclusionary rule substantially reduces any remaining motivation the government has for ensuring data quality as it gives the government, through its law enforcement agents, unfettered permission to use incorrect information, albeit in good faith, to obtain faulty warrants, to perform unreasonable searches and seizures, and to interfere with one's liberty without instilling any incentive to correct the underlying system of information on which these actions are based.

This article explores some of the critical issues surrounding the government's use of information and the data quality standards that are applied. In particular, this article focuses on the failure of the government and the legal system to adequately address the quality of data that it cascades and shares in pursuit of national security. This article will illustrate how other motivations to ensure data quality such as redress, statutory compulsion, internal audit, and mission-related activities do not seem to be effective as they can be waived, repeatedly violated, and oft ignored. Section II surveys various watch lists and databases, the current state of their data quality, and the methods employed for ensuring data quality. Section III reviews the legislation on data quality and privacy protections and its failure to adequately assign responsibility and enforcement for data quality. Section IV examines the Supreme Court's holding in *Herring* and its impact on data quality standards. Section V offers recommendations for assigning responsibility and enforcing data quality standards for information used to support national security. These recommendations attempt to strike a balance between the need to leverage watch lists and databases to share information on national security issues while protecting our fundamental protections guaranteed under the Constitution.

II. WATCH LISTS AND THE QUALITY OF DATA

Once information is placed in an electronic database or other information system, the human tendency is to accept the accuracy of that in-

6. U.S. CONST. amend. IV.

7. U.S. CONST. amend V.

8. Herring v. United States, 129 S. Ct. 695, 702-04 (2009).

formation without question.[9] This phenomenon is not limited to electronic databases; it can be observed in our willingness to believe print sources on their face as well.

Because this article focuses on the responsibility for data quality, a definition of data quality and what it entails is a logical starting point. Data quality has been defined according to three key terms: "objectivity," "utility," and "integrity."[10]

> "**Objectivity**. . . ensures disseminated information, as a matter of substance and presentation, is accurate, reliable, and unbiased."[11]

> "**Utility** requires that the "usefulness of the information" is assessed. This assessment includes "continuously monitoring information needs and developing new information sources or revising existing methods, models, and information products where appropriate."[12]

> "**Integrity**. . . ensures information is protected from unauthorized access, corruption, or revision."[13]

Those charged with managing information must put policy, process, and tools in place to control and monitor the data quality.

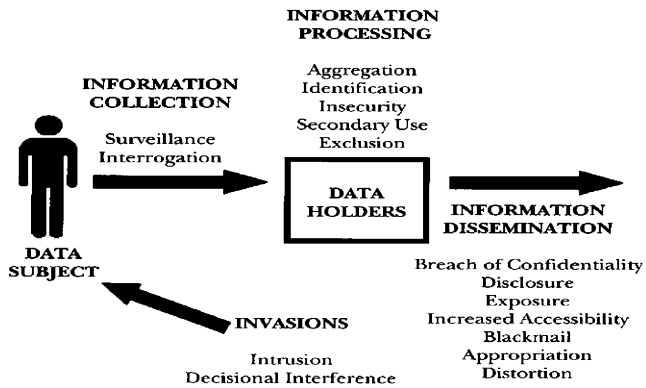

Figure 1: Model depicting the elements of the taxonomy of privacy as described by Solove.[14]

---

9. P. STEPHEN GIDIERE III, THE FEDERAL INFORMATION MANUAL, HOW THE GOVERNMENT COLLECTS, MANAGES, AND DISCLOSES INFORMATION UNDER FOIA AND OTHER STATUTES 176 (2006).

10. PATRICE MCDERMOTT, WHO NEEDS TO KNOW? THE STATE OF PUBLIC ACCESS TO FEDERAL GOVERNMENT INFORMATION 239 (2007).

11. United States Department of Justice, *Department of Justice Information Quality Guidelines*, http://www.usdoj.gov/iqpr/dojinformationqualityguidelines.htm (last visited Apr. 18, 2009).

12. *Id.*

13. *Id.*

14. DANIEL J SOLOVE, UNDERSTANDING PRIVACY 104 (2008). Figure 1 is taken in its entirety from Solove's *Understanding Privacy*.

As shown in Figure 1, "[t]he general progression from information collection to processing to dissemination is the data moving further away from the individual's control."[15] Therefore, it seems inappropriate to put the onus on the data subject or person to ensure that the information collected, processed, and disseminated about them remains accurate. This duty, as illustrated in Figure 1, centers on the data holders – those that can directly control the data quality. As Edward Deming observed, "[eighty-five percent] 85% of poor quality is directly attributable to the manufacturing process and only [fifteen percent] 15% to the [individual] worker" producing a product.[16] It is, therefore, reasonable to believe that the processes used to collect, process, and disseminate ("manufacture") information, as illustrated in Figure 1, are where the majority of the data quality errors are introduced.

A. Watch Lists and Databases

As defined by the *Oxford English Dictionary*, a "watch list" is "a compilation of items or names that require close surveillance, especially for legal or political reasons."[17] Watch lists maintained by the government address a wide range of categories and have broad impact on the lives of individuals contained in the lists, including whether they can travel via airplane, obtain employment, and the like. Table 1, shown below, provides a summary of some of the watch lists maintained by federal agencies in support of national security.

B. Data Quality of the Watch Lists

In May 2009, the Office of Inspector General ("OIG") for the Department of Justice released the findings of its audit on the nomination process for the Terrorist Watch List[18] maintained by the Federal Bureau of Investigation ("FBI"). This particular watch list was established to "develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."[19]

---

15. *Id.* at 103.

16. Ranjit K. Roy, A Primer on the Taguchi Method 8 (1990).

17. Shorter Oxford English Dictionary 3589 (5th ed. 2002).

18. Homeland Security Presidential Directive 6: Directive on Integration and Use of Screening Information to Protect against Terrorism, 39 Weekly Comp. Pres. Doc. 1234 (Sept. 16, 2003). The Terrorist Watch List was established through the Homeland Security Presidential Directive 6, issued by President George W. Bush in 2003. *Id.*

19. *Id.*

Dept	Agency	List	Purposes	Further Background
State	Bureau of Consular Affairs	Consular Lookout & Support System	Vetting foreign nationals seeking visas	Receives information from TIPOFF
	Bureau of Intelligence and Research	TIPOFF	Tracking known and suspected international terrorists	Created in 1987, transferred to Terrorist Threat Integration Center (TTIC) in 2003 and then to the National Counterterrorism Center (NCTC) in 2004, which now maintains the Terrorist Identities Datamart Environment watch list for international terrorists
Homeland Security	U.S. Customs and Border Protection	Interagency Border Inspection System	Primary database for border management and Customs law enforcement	Part of Treasury Enforcement Communications System (TECS)
	Transportation Security Agency (TSA)	No Fly List	Identify threats to civil aviation	Names added by FBI case agents and NCTC analysts
		Selectee List	Selecting passengers for additional screening	Provided to airlines on a daily basis
	U.S. Immigration and Customs Enforcement	National Automated Immigration Lookout System	Biographical and case date for aliens who may be inadmissible in US	Created originally by [Immigration and Nationalization Service] INS, now absorbed into [Department of Homeland Security] DHS systems in 2005, also housed in TECS
		Automated Biometric Identification System	Tracking aliens entering US illegally or suspected of crimes	Created by INS, transferred to DHS in 2003

Justice	U.S. Marshals Service	Warrant Information Network	Tracking persons with existing federal warrants	Does not perform any independent watch list function regarding terrorism
	FBI	Violent Gang and Terrorist Organization File	Tracking individuals associated with gangs and terrorist organizations	Created in 1995 as a component of the National Crime Information Center [NCIC]
		Integrated Automated Fingerprint ID System [IAFIS]	National fingerprint and criminal history database	Supplies biometric identifying information to support other watch lists
	U.S. National Central Bureau of Interpol	Interpol Terrorism Watch List	Assistance for global police operations	Created in 2002; contains about 100 names also in other watch lists
Defense	Air Force Office of Special Investigations	Top 10 Fugitive List	Retrieving Air Force fugitives	Performs no independent terrorist watch list function

Table 1: Summary of Some Watch Lists Maintained by Federal Agencies.[20]

"This list is primarily used by frontline screening personnel at U.S. points of entry and by federal, state, local, and tribal law enforcement."[21] The May 2009 audit report is a report of the audit performed in March 2008 where the OIG determined "that the initial watch list nominations created by FBI field offices often contained inaccuracies or were incomplete" and "that the FBI did not consistently update or remove watch list records, when appropriate."[22]

As of September 2008, it was estimated that there were more than 400,000 unique individuals on the Terrorist Watch List.[23] This report makes note of several data quality issues related to the Terrorist Watch List.

20. Peter M. Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804, 813 tbl.1 (2007). Table 1 was taken in its entirety from Shane's article.

21. U.S. DEPART. OF JUSTICE OFFICE OF THE INSPECTOR GEN. AUDIT DIVISION, THE FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES, AUDIT REPORT 09-25, i (May 2009), *available at* http://www.justice.gov/oig/reports/FBI/a0925/final.pdf [hereinafter AUDIT REPORT].

22. *Id.* at ii.

23. *Id.* at ii n.4.

> In [sixty-seven] 67 percent of the cases where a watch list record modification was necessary, the FBI failed to modify the watch list record when new identifying information was obtained during the course of the investigation, as required by FBI policy.[24]

> In [seventy-two] 72 percent of the closed cases reviewed, the FBI failed to remove the subject in a timely manner.[25]

Some of these errors introduce risk to national security, but they also introduce situations where the individuals whose data is incorrect or who have not been appropriately removed from the watch list are delayed or inconvenienced. In the report, the OIG notes that nearly fifteen percent of the individuals who should have been removed from the watch list were unnecessarily delayed by frontline personnel more than six times.[26]

Interestingly, even though these individuals could have filed a redress[27] complaint through the Department of Homeland Security ("DHS") Traveler Redress Inquiry Program[28] ("TRIP"), none of them had done so as of September 2008.[29] DHS TRIP allows individuals to seek some form of relief from being stopped unnecessarily or misidentified as a result of a watch listing.[30] Requests received through TRIP are routed for redress to the appropriate DHS components.[31] The appropriate department reviews the request and reaches a determination about an individual's status.[32] If redress is granted, the results are recorded in another system to allow the airlines to prevent future delays for misidentified individuals until the watch list is corrected.[33]

C. Methods for Ensuring Data Quality

While inspection is a good tool in monitoring the quality of the information in the various watch lists and databases, "no amount of inspection can put quality back into [a] product – it is merely treating a

---

24. *Id.* at iv.

25. *Id.* at iv-v.

26. *Id.* at 41.

27. Redress is a process by which the affected party can request to have data corrected, updated, or removed and, in some cases, can request damages for the harm caused by the misinformation.

28. Transportation Security Administration, *DHS Traveler Redress Inquiry Program,* http://www.tsa.gov/travelers/customer/redress/index.shtm (last visited Mar. 20, 2009) [hereinafter TSA]. The form to submit for inquiry and redress is available at, http://www.dhs.gov/xlibrary/assets/DHSTRIP_Traveler_Inquiry_Form.pdf, (last visited Mar. 20, 2009).

29. Audit Report, *supra* note 21, at 41.

30. TSA, *supra* note 28.

31. *Id.*

32. *Id.*

33. *Id.*

symptom."[34] Even though the results in the 2009 OIG audit are somewhat improved over the results from the 2008 audit,[35] there are still numerous data quality issues. It is a generally held principle in quality management that quality cannot be improved simply by inspection;[36] therefore, it is unlikely that audits and inspections alone will improve the quality of the data in watch lists and national security databases. It will require both inspections and a concerted effort during the front end of the data collection and processing to ensure continued quality of the data.

There are no published criteria for including an individual on a watch list.[37] This lack of criteria also means there is no prior notice as to when or why someone is added to a watch list[38] and there is no opportunity to challenge the inclusion.[39] The first time an individual knows that he or she is on a watch list is when they are denied some privilege, such as airline travel. This places the emphasis on the individual rather than the data holder to identify the data quality issue and have it corrected.

Once an individual attempts to correct false or inaccurate information, the processes available to the individual require him to know the information holder who included the information initially so the error can be corrected at its source. However, since the information in these systems does not contain attribution,[40] or rather a full history of where the information was obtained or entered into the system, the ability to correct the information at the right location and ensure it cascades to all constituent databases is difficult at best. It is particularly onerous for the individual that has little to no insight into the process by which the information was included.

III. LEGISLATIVE POSTURE FOR DATA QUALITY OF NATIONAL SECURITY INFORMATION

As Solove noted in his book, *Understanding Privacy*, information maintained by the government can be used to make important decisions about people's lives.[41] The individual whose life can be shaped by this information has scant knowledge of how the information has been col-

34. ROY, *supra* note 16, at 8-9.

35. AUDIT REPORT, *supra* note 21.

36. ROY, *supra* note 16, at 8-9.

37. Daniel J. Steinbock, *Designating the Dangerous: From Blacklists to Watch Lists*, 30 SEATTLE U. L. REV. 65, 81 (2006).

38. *Id.* at 96.

39. *Id.* at 93.

40. Paul Rosenzweig & Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum*, 17 LEGAL MEMORANDUM, June 17, 2005, at 11-12, *available at* https://www.policyarchive.org/bitstream/handle/10207/8408/lm_17.pdf.

41. SOLOVE, *supra* note14, at 182.

lected, processed, and used, and this information is unfortunately often subjected to a bureaucratic process that lacks discipline and control.[42] There are several laws to provide access to this information and to provide mechanisms to ensure the quality of this information. It is the implementation of these laws where the challenge seems to lie.[43] The following is a summary of those laws and some of the drawbacks in their implementation as it relates to monitoring and enforcing quality in watch lists and national security information as it applies to the individual.

A. Privacy Act

Around the world there are various rights for people to access and correct their records – whether they are governmental records, health records, personnel records, or the like.[44] Providing such mechanisms can be costly and time consuming, but failure to do so can erode accountability on the part of government agencies and businesses that maintain records about individuals.[45] The Privacy Act of 1974[46] generally allows a United States citizen to gain access to most personal information maintained by Federal agencies and to be able to correct any inaccurate, incomplete, untimely, or irrelevant information.[47] The Privacy Act does not apply to every record for an individual,[48] but rather the Act only applies to those records held by an "agency," as defined by the Act.[49] Therefore, the records held by courts, executive components, or non-agency governmental entities are not subject to the provisions in the Privacy Act. An individual has no right to these records, or at least no right protected by Congressional statute.[50] While the Computer Matching and Privacy Protection Act of 1988[51] amended the Privacy Act by adding certain protections for subjects of Privacy Act records whose records are used in automated matching programs, it did not expand the protections

42. *Id.*

43. McDermott, *supra* note 10, at 255.

44. *E.g.*, Freedom of Information Act, 5 U.S.C § 522 (2004) (U.S.); The Freedom of Information Act, 1989, Aust. Cap. Terr. Laws 46, (Austl.), *available at* http://www.legislation.act.gov.au/a/alt_a1989-46co/default.asp.

45. Solove, *supra* note14, at 134.

46. 5 U.S.C. § 552a.

47. Comm. on Gov't Reform, A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records, H.R. Rep. No. 108-172 (2005), at 25, *available at* http://www.fas.org/sgp/foia/citizen.pdf [hereinafter Citizen's Guide].

48. Privacy Act of 1974, 5 U.S.C. § 552 (2004).

49. *Id.*

50. *See* Dale v. Executive Office of the President, 164 F. Supp. 2d 22, 25 (D.D.C. 2001).

51. Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (2004).

to all of the places those electronic records were shared as part of automated matching programs.

To initiate a Privacy Act request, the requester must identify either the specific system of records or the agency responsible for the records the requester wishes to obtain.[52] Each agency provides details on how to request records under the Privacy Act. The requester must then write a letter requesting the information.[53] The letter must contain: 1) a statement that the request is being made under the Privacy Act provisions; 2) the name, address, and signature of the requester; and 3) a description of the records being requested.[54] This first letter is needed to obtain access to the records.[55] A second letter is needed to make corrections to the record.[56] Again, the letter requesting the correction will normally be sent to the agency that maintains the record in question.[57] The letter to request a correction to a record must: 1) request a record to be amended under the provisions of the Privacy Act; 2) identify the specific record and specific information in the record to be corrected; 3) state why the information is incorrect, untimely, irrelevant, or incomplete; 4) identify any new or additional information that should be included in place of the erroneous information; and 5) provide the name, address, and telephone number of the requester.[58] While the Internet has improved access to information on the request process, it is still a very cumbersome process for the individual to identify the appropriate system of record and to submit the request to the appropriate agency.

Once the request is submitted, the Privacy Act provides time limits that should be met when responding to a request, providing notification to the requester, and formalizing an appeal process.[59] However, there is an exception whereby the agency can determine its own timeline for actually making a correction if one is deemed appropriate.[60]

The Privacy Act has two general exemptions: 1) all records maintained by the Central Intelligence Agency and 2) selected records maintained to support criminal law enforcement.[61] There are three types of criminal law enforcement records that are exempt.[62] Specifically, one type is information compiled regarding the criminal history of an individ-

52. CITIZEN'S GUIDE, *supra* note 47, at 25.
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.* at 31.
57. *Id.*
58. CITIZEN'S GUIDE, *supra* note 47, at 31-32.
59. 5 U.S.C. § 552(a)(6).
60. GIDIERE, *supra* note 9, at 66.
61. CITIZEN'S GUIDE, *supra* note 47, at 28.
62. *Id.*

ual.[63] In addition to the general exemptions, the Privacy Act provides for seven specific exemptions.[64] One of these exemptions in particular expands upon the law enforcement general exemption by providing exemption for records containing investigative material used by law enforcement for purposes other than those covered by the general exemption.[65] This specific exemption is limited, however, and disclosure of the records is required if, as a result of the record, an individual would be denied any right, privilege, or benefit to which he or she would be entitled under Federal law.[66] Such exemptions make the Privacy Act virtually irrelevant for allowing the individual to monitor information on his or her criminal record and to make corrections if appropriate.

B. Freedom of Information Act

The Freedom of Information Act ("FOIA")[67] provides that any person has the right to request access to federal agency records of information. The Act requires all agencies of the Executive Branch to disclose records when a written request is received unless the information requested is one of nine categories of records that are exempt.[68] There is no central department or office that responds to all information requests; instead, each agency has its own office to respond to requests for its own records.[69] This requires the person making the request to know which agency has the records in question and that agency's process for requesting those records.[70] In addition, the requester may have to pay a fee for the processing of the request.[71] If the request is for personal information regarding the requester, the requester will either be asked to supply a notarized statement authorizing the release of the information or a statement, signed under penalty of perjury, that the requester is who he says he is.[72] In some cases, a Privacy Act request may return more information than a FOIA request.[73] Generally, FOIA requests must be

63. *Id.*

64. *Id.* at 29-30.

65. *Id.* at 29.

66. *Id.*

67. 5 U.S.C § 522.

68. Dep't of Justice, Freedom of Information Act Reference Guide (2006), http://www.justice.gov/oip/referenceguidemay99.htm [hereinafter FOIA Guide].

69. *Id.*

70. However, a requester who does not know which specific agency holds the records may be provided with a government directory and may make a request to multiple agencies. Citizen's Guide, *supra* note 47, at 9.

71. Citizen's Guide, *supra* note 47, at 11.

72. FOIA Guide, *supra* note 68.

73. *Id.*

processed in a specific timeframe, currently twenty days,[74] but depending on the scope and complexity of the request, the agency can provide an alternate timeframe.[75]

As mentioned, there are nine statutory exemptions to FOIA.[76] This includes an exemption for law enforcement that "allows agencies to withhold law enforcement records in order to protect the law enforcement process"[77] and procedures if the disclosure of such information would reasonably risk circumvention of the law, interfere with an investigation, or endanger the life or physical safety of an individual.[78] This generally means that any information related to a person's current status in regard to law enforcement, such as outstanding warrants, criminal record, and the like can be exempt from FOIA and Privacy Act requests at the discretion of the agency in possession of those records. While the intent of FOIA, and indeed the Privacy Act, is to provide access to government information, it is difficult to fully comprehend the information sources[79] and to make a meaningful request to the right agency for the right information in order to get the desired results.

C. Information Quality Act

In 2000, Congress enacted the Data Quality Act[80] to establish administrative mechanisms to allow "affected persons to seek and obtain correction of information maintained and disseminated by the agency."[81] The Data Quality Act[82] requires the Office of Management and Budget ("OMB") to issue government-wide guidelines for ensuring the quality, objectivity, utility, and integrity of information, including specifically statistical information, disseminated to the public by Federal agencies.[83] As noted by the Department of Justice's guidelines for ensuring data quality, the guidelines are not a regulation and are not legally enforceable nor do the guidelines "create any legal rights or impose any legally

74. *Id.* This response requirement was enacted in the 1996 amendments to FOIA and became effective in October 1997 – codified at 5 U.S.C. § 552(6)(A)(i), as amended by Public Law No. 104-231, 110 Stat. 3048.

75. *Id.*

76. *Id.*

77. Citizen's Guide, *supra* note 47, at 18.

78. *Id.* at 18-19.

79. McDermott, *supra* note 10, at 256.

80. The Data Quality Act, 44 U.S.C. § 3516 (2000).

81. *Id.* at § 3516(b)(2)(B); s*ee also* Gidiere, *supra* note 9, at 62.

82. 44 U.S.C. § 3516. The Data Quality Act was enacted as part of a rider in a spending bill so it was not given a name in the actual legislation. The Government Accountability Office calls it the Information Quality Act, while others call it the Data Quality Act.

83. *Id.* at § 3516(a).

binding requirements or obligations on the agency or the public."[84] In addition, the guidelines do not apply to information disseminated by "intra-or inter-agency use or sharing of government information."[85]

Two federal courts have been provided with the opportunity to review claims under the Information Quality Act and both held that the Act's "broad directive does not provide a meaningful standard for court review."[86] As compared to the Privacy Act's correction capability that allows for redress[87] and allows a court to review an agency's final decision,[88] the Information Quality Act does not provide enough standards by which to judge an agency's decision or to determine if the plaintiff was able to demonstrate standing. So, like the Privacy Act and FOIA, the Data Quality Act does not provide adequate ability for an individual to monitor and correct information that would be contained in watch list, criminal record, or national security databases. In addition, the current legislation does not provide adequate incentives for the government agencies to maintain the quality of this data, because they are largely exempted from the data quality and fair practices in information standards.

D. Fair, Accurate, Secure, and Timely (FAST) Redress Act of 2009 – Pending legislation

The House has introduced a bill, *FAST Redress Act of 2009*, to establish an appeal and redress process for individuals wrongly delayed or prohibited from boarding a flight, or denied a right, benefit, or privilege.[89] If passed, this bill would establish the creation of a "Comprehensive Cleared List" for individuals who were misidentified, completed an appeal and redress request, and permitted the use of their personally identifiable information to be shared between departmental entities.[90] This bill has passed the House and has been referred to the Senate Committee on Commerce, Science, and Transportation. According to the Congressional Bills Legislative Forecasts Current Congress, House Bill 559 has a fifty percent chance of passing the Senate Committee and a twenty-five percent chance of passing the Senate Floor.[91] *BillCast*[92]

84. *See* United States Department of Justice, *Department of Justice Information Quality Guidelines*, http://www.usdoj.gov/iqpr/dojinformationqualityguidelines.htm (last visited Apr. 18, 2009).

85. *Id.*

86. Gidiere, *supra* note 9, at 68.

87. 5 U.S.C. §§ 552a(g)(1)(C) & (g)(4).

88. Gidiere, *supra* note 9, at 69.

89. FAST Redress Act of 2009, H.R. 559, 111th Cong. (2009).

90. *Id.*

91. *Congressional Bills Legislative Forecasts* is available through the BLCAST database on LexisNexis.

gives House Bill 559 a twenty-four percent chance of passing the Senate. Unfortunately, even if passed, this bill is limited to terrorist watch lists and does not provide redress for the other information exempted from the Privacy Act and FOIA.

IV. TO EXCLUDE OR NOT TO EXCLUDE – IMPACT OF *HERRING* ON DATA QUALITY

While the Fourth Amendment protects an individual from unreasonable searches and seizures,[93] there are no specific provisions for what happens to the evidence obtained under an unreasonable search or seizure.[94] The *exclusionary rule* is a judicially created rule that suppresses the introduction of illegally obtained evidence at a criminal trial.[95] The exclusionary rule is, therefore, intended to provide a mechanism to safeguard the protections in the Fourth Amendment by deterring misconduct on the part of law enforcement.[96] Even so, the exclusionary rule is not a guaranteed right in every unreasonable search and only applies when the exclusion of the evidence would result in "appreciable deterrence."[97] As defined in *Leon*, the benefit of excluding the evidence must outweigh the cost of letting potentially guilty people go free.[98]

In *Herring*, the court held that the exclusionary rule does not apply if the evidence obtained from a search was the result of isolated negligence.[99] In *Herring*, the mistake made by the police was based on an error in a database that showed Herring had an outstanding warrant, which resulted in his arrest and search.[100] The court determined that since the police acted in good faith based on the information they had at the time and the error was due to a data entry mistake by the county warrant clerk, the exclusionary rule should not apply and the results of the search should be admissible.[101]

The court in *Herring*, following the rule in *Leon*, focused on the use of the exclusionary rule as a deterrent when mistakes were made in the

92. *BillCast* provides forecasts for legislation and is available through the BC database on WestLaw.

93. U.S. CONST. amend. IV.

94. *Herring*, 129 S. Ct. at 699.

95. *Id.*; *see also* Potter Stewart, *The Roadmap to Mapp v. Ohio and Beyond: The Origins, Development, and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1372 (1983).

96. *Herring*, 129 S. Ct. at 699.

97. United States v. Leon, 468 U.S, 897, 909 (1984).

98. *Leon*, 468 U.S. at 922.

99. *Herring*, 129 S. Ct. at 698-99.

100. *Id.* at 698.

101. *Id.* at 698-04.

databases that affected the arrest and search processes. The court, however, did not focus on the systemic nature of the errors in the underlying information and whether it was prudent of law enforcement to rely exclusively upon that information. In this case, the error remained undetected in the system for over five months.[102] In *Herring*, the court stated that the exclusionary rule serves to "deter deliberate, reckless, or grossly negligent conduct or in some circumstances recurring or systemic negligence"[103] and the court did not feel the circumstances in *Herring* rose to that level.[104] However, it can be argued that, given the reportedly large number of errors in the data on which law enforcement relies in the criminal records and watch lists, these errors are systemic and reoccurring and demonstrate gross negligence on the part of the data holder. It follows then that, without the exclusionary rule, there is no incentive for the police or other data holders or data consumers to ensure that data is accurate before they act upon it.

The court in *Herring* stated that if the police had been shown to be reckless in maintaining a warrant system, the exclusionary rule would "certainly be justified."[105] Taking this point further raises the question of whether failing to ensure the accuracy of the data in the warrant system, by any of the actors responsible for its maintenance, would not also be reckless, and therefore, the exclusionary rule would apply. This is similar to the argument raised by the dissent in *Herring* in which Justice Ginsburg, quoting the dissent in *Arizona v. Evans*, stated that the serious impact of the court's decision in *Herring* will have on the innocent people who are "wrongfully arrested based on erroneous information [carelessly maintained] in a computer database."[106] Justice Ginsburg further elaborated that the inaccuracies in expansive, interconnected repositories of information can raise concerns regarding individual liberty.[107] Justice Ginsburg went on to state that the exclusionary rule can be viewed as a way to provide a constraint on the power of the government, not just some of its agents.[108] Instead of applying the multi-factor, case-by-case test for police culpability that the court in *Herring* adopted, Justice Ginsburg recommended the applying the exclusionary rule whenever law enforcement personnel is responsible for errors in databases that result in a Fourth Amendment violation.[109]

---

102. *Id.* at 705.

103. *Id.* at 702.

104. *Herring*, 129 S. Ct. at 702.

105. *Id.* at 703.

106. *Id.* at 705 (Ginsburg, J., dissenting) (quoting Justice Stevens' dissent in Arizona v. Evans, 514 U.S. 1, 22 (1995)).

107. *Id.* at 709.

108. *Id.* at 707. *See also* STEWART, *supra* note 95.

109. *Herring*, 129 S. Ct. at 711 (Ginsburg, J., dissenting).

Unlike the majority opinion in *Herring*, Justice Ginsburg's recommendation recognizes that, in this age of almost exclusive reliance on information sharing, reckless and negligent actions of law enforcement are not limited to its agents on the street but rather to the law enforcement system in its entirety. Officers and agents can indeed act in good faith based on the information they are provided. However, when that information is faulty, through no direct action of the officer on the street, but rather through careless practices and systemic negligence, the resulting action is no less harmful to the rights of the individual than if the officer had acted recklessly.

V. RECOMMENDATIONS FOR ASSIGNING RESPONSIBILITY AND ENFORCEMENT FOR DATA QUALITY

If the government becomes a lawbreaker, it breeds contempt for the law; it invites every man to become a law unto himself; it invites anarchy.[110]

As Solove noted, if government can promise confidentiality (and integrity) of data but suffer no consequences for violating its words, then such promises become unreliable and erode the trust of the government and the information.[111] This need for trust is reiterated in Shane's article where he states that when "the unjustified targeting of innocent persons becomes widespread, the very fabric of mutual confidence between citizen and government. . . would be threatened."[112] To ensure the quality of data the government uses in support of national security will require a comprehensive program so that quality can be built into, and maintained within, the national security databases and watch list processes. This program will need to rely on people, process, and technology as has been outlined in other privacy protection legislation[113] for such areas as medical and banking information.

A. Reduce Exemptions from Legislative Requirements

As discussed in Section III, the legislative posture and protections are somewhat weak or non-existent when it comes to enforcing data quality on the criminal law enforcement and national security watch lists and databases because these are exempt from the protections offered by the Privacy Act, FOIA, and the Data Quality Act. The prognosis for House Bill 559 is not very good and even if passed would only provide a redress capability after the harm is already done. To date, there are no

110. Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting).

111. Solove, *supra* note 14, at 182.

112. Shane, *supra* note 20, at 808.

113. Examples of this legislation include the Gramm-Leach-Bliley-Act (GBLA), Pub. L. 106-102, 113 Stat. 1338 (1999) and the Health Insurance Portability and Accountability Act (HIPAA), Pub, P. L. 104-191, 110 Stat. 2021-2031 (1996).

legislative protections that would provide an individual with the opportunity to monitor and correct information or misidentification before the harm is realized. Additional legislation should be considered to either amend the exemptions or provide specific access and correction capability for individuals to monitor the information contained about them in national security databases and watch lists. This ability to monitor could be limited to that information that would deny the individual a right, benefit, or privilege so long as that information is not part of an active investigation or would expose sensitive national security procedures. However, the government's ability to claim such privilege would need to be scrutinized.[114] In addition, the legislation should include a requirement to report to Congress on the state of the watch lists, like the number of people on the lists, the criteria for inclusion on the lists, the number who have challenged their inclusion, and the disposition of any redress.[115] This type of reporting would provide insight into the extent of the redress issue and may suggest future enhancements to the data quality for the watch list and other national security programs. As Shane noted, "it ought to be viewed as intolerable in a democratic society for large numbers of innocent people to be stigmatized by the government under a largely secret program, even if such cases can be redressed through post-inclusion individual review."[116]

B. Increased Requirements for Internal Agency Controls

As previously noted, quality cannot be inspected into data. In addition to a recommendation to increase legislation to provide for accuracy, accountability, and redress, internal agency controls must be enhanced as well. Enhancements to the internal agency controls should include both front-end controls to address data collection and processing as well as back-end controls, such as redress, to handle situations where data is incorrect. To date, much of the internal controls have been focused on redress. While some redress programs, such as the one for the United States Visitor and Immigrant Status Indicator Technology ("US_VISIT"), have been markedly successful,[117] redress will only protect those individuals who become aware that they are listed.[118]

Providing controls on the processes to collect data and incorporate that data into watch list and national security databases' cascade of in-

114. This topic is too complex to cover in this paper. For coverage of the government's alleged misuse of the claim of privilege surrounding national security issues, s*ee* Barry Siegel, Claim of Privilege: A Mysterious Plane Crash, a Landmark Supreme Court Case, and the Rise of State Secrets (2008).

115. Shane, *supra* note 20, at 854.

116. *Id.* at 809-10.

117. *Id.* at 847.

118. *Id.* at 821.

formation is critical. These controls would help to ensure that the initial data going into these systems was accurate at the outset. In addition, internal quality controls will require regular sampling of records to determine whether the information has been accurately recorded and whether the information is consistent about individuals as it is cascaded to other systems or databases.[119]

In addition to the controls to ensure the accuracy of the information, it is also important to monitor the integrity of the information to ensure that no unauthorized modifications have been made. In *Herring*, it took five months to determine that incorrect information was retained in the database. It seems unlikely that there were processes in place to monitor unauthorized access or modifications to the records in the same database. Implementing information security practices and audit trails will help to identify responsibility for records and to provide traceability of each record's origin and modification during its lifecycle.

Another important element is training for the various parties that interact with the watch lists and databases to ensure they are aware of, and adhere to, defined quality controls throughout the information collection, processing, and dissemination processes as reflected in Solove's taxonomy.[120] In interviews with case agents, who are the primary interface with the terrorist watch list nomination process, the OIG noted that "some case agents did not consider watch list record removal to be a high priority and they did not always understand the ramification of untimely removals."[121] The audit report went on to conclude that "[s]ome case agents did not appear to understand that the watch list is disseminated to other organizations. Therefore, these case agents did not recognize that the watch listed individuals or others with similar names could be delayed, detained, or otherwise inconvenienced by law enforcement and screening personnel."[122]

C. Exclusion of Evidence

The exclusion of evidence is a powerful incentive to ensure that law enforcement actions are handled appropriately. While the isolated error referenced in *Herring* may not rise to the level of deterrence required by the exclusionary rule, it is clear that the court in *Herring* has left the door open to exclude evidence in situations where the errors were reckless, negligent, and systemic.[123] Suggesting, as the courts have done in prior exclusionary rule cases, such as *Evans* and *Herring*, that excluding

119. *Id.* at 829.
120. Solove, *supra* note 14.
121. Audit Report, *supra* note 21, at 42.
122. *Id*. at 42.
123. *Herring*, 129 S. Ct. at 704.

evidence would not deter the carelessness of other government entities,[124] runs counter to the principles underlying negligence law.[125]

Given the data quality issues discussed in this article, it is recommended that evidence resulting from errors in watch lists and national security databases should be excluded when the evidence is obtained through violations of the Fourth Amendment. In addition to the recommended enhancements to legislative and internal controls, use of the exclusionary rule would go some way in providing a strong incentive to the various data holders and data consumers to ensure the quality of the data they manage throughout its lifecycle – from the information's initial collection and inclusion in a database to the removal of the information when it is no longer valid or relevant. Such exclusions would fill the gap when fair information practices noted in legislative requirements can be exempted for law enforcement purposes. Further, such exclusions would instill an incentive to the government agencies to maintain all the records they use in making decisions about individuals with "accuracy, relevance, timeliness, and completeness" in order to ensure fairness to the individuals affected.[126]

VI. CONCLUSION

Perhaps the idea that with great power comes great responsibility[127] has become too cliché in our society and is oft misused. However, in 1995, Justice O'Connor observed a similar concept in her concurring opinion in *Arizona v. Evans*, "[i]n recent years we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. . .With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities."[128] When so much of our liberty rests on the quality of the data in the databases and watch lists that the government uses for national security, it is irresponsible to allow such systems to be exempt from legislatively mandated data quality standards and enforcement. While it offers some relief, being able to correct an error in a database or watch list only after an innocent person is drawn into an adverse event, such as being wrongfully arrested, detained, prevented from flying, or subjected to humiliating treatment, is too little and too late.

---

124. *Id.* at 704; *Evans*, 514 U.S. at 28-29.

125. *Herring*, 129 S. Ct. at 704.

126. 5 U.S.C. § 552a(e)(5) (2004).

127. Phrase used by character *Benjamin Parker* in SPIDERMAN (Columbia Pictures 2002).

128. *Evans*, 541 U.S. at 17-18.

Given the increased technology and the state of information sharing under the auspices of national security, perhaps this is the best and most appropriate time to remind our government of its inherent responsibilities – to ensure the quality of the cascading information it shares in order to sustain the very protection of the citizens, residents, and visitors it purports to serve. When the government fails to meet its responsibility for ensuring this quality, simple redress for the error and the damages it may cause is not enough. The government must endure the sanction imposed upon it under the exclusionary rule – for it is a constraint on the power of the government as a whole and not just some of its agents[129] to preserve our fundamental protection under the Fourth Amendment to be secure in our persons, houses, papers, and effects.

129. *See Herring*, 129 S. Ct. at 707 (Ginsburg, J., dissenting).