Kafkaesque Dangers: IPERIA, Do Not Pay, and the Government's New Fight Against Improper Payments

Bryan Reece Clark[*]

ABSTRACT: The Do Not Pay Initiative ("Do Not Pay") is a government program designed to help government agencies identify and eliminate the improper payment of federal funds. A payment is considered improper when: (1) an incorrect amount is paid to an eligible recipient; (2) it is made to an ineligible recipient; (3) it is for goods or services not received; (4) it is a duplicate payment; or (5) there is insufficient or no documentation supporting the payment. Do Not Pay helps eliminate improper payments by conducting automated investigation activities into agency payee data through computer matching algorithms and advanced analytics. Do Not Pay provides the results of these investigations to government agencies, allowing them to make payee eligibility decisions. However, the Privacy Act of 1974 initially restricted the ability of government agencies to use Do Not Pay's full computer matching capabilities, which involve matching on personal information. In 2012, Congress broke down this restriction by passing the Improper Payments Elimination and Recovery Improvement Act of 2012 ("IPERIA"). IPERIA ushers in a new era of administrative efficiency in agency access to Do Not Pay's full computer matching capabilities. Yet this new era raises important policy concerns for individual privacy, precisely as more agencies conduct enhanced automated investigation of their payees.

I. INTRODUCTION 1720

II. IMPROPER PAYMENTS AND THE DO NOT PAY INITIATIVE 1723
A. *WHAT ARE IMPROPER PAYMENTS?* 1723
B. *THE GOVERNMENT ESTABLISHES THE DO NOT PAY INITIATIVE* 1725

[*] J.D. Candidate, The University of Iowa College of Law, 2017; M.B.A. Management, Rockhurst University, 2013; B.A. Economics, Political Science, Rockhurst University, 2011. I would like to thank my wife Katelyn for her love and support, my family for their continued encouragement, and all of the talented individuals on the *Iowa Law Review*. I dedicate this Note to my late father, Dick Clark, who is greatly missed by friends and family.

C. DO NOT PAY INITIATIVE RESULTS AND CHALLENGES 1728

III. IMPROPER PAYMENT ELIMINATION AND RECOVERY IMPROVEMENT ACT 1733
A. THE PURPOSE OF IPERIA 1733
B. BALANCING ADMINISTRATIVE EFFICIENCY AND INDIVIDUAL PRIVACY INTERESTS 1736
1. IPERIA Falls Squarely Within the Kafkaesque Paradigm .. 1739
2. IPERIA Mitigates Kafkaesque Dangers, but Concerns Remain 1744

IV. OMB SHOULD ISSUE ADDITIONAL GUIDANCE 1747
A. INCREASE DATA INTEGRITY BOARD EFFECTIVENESS ON THREE FRONTS 1748
1. Semiannual Board Meetings 1748
2. Interagency Knowledge Sharing 1749
3. Strategic Planning 1750
B. ESTABLISH ANNUAL RECERTIFICATION REQUIREMENTS FOR THE DATA INTEGRITY BOARDS 1751
C. REQUIRE DATA INTEGRITY BOARDS TO SELF-ASSESS THEIR EFFECTIVENESS WITH THE PRIVACY OFFICER 1752
D. DEFINE WHAT "SUFFICIENTLY SIMILAR" MEANS IN THE CONTEXT OF DATA ELEMENTS 1754

V. CONCLUSION 1756

I. INTRODUCTION

"*The only thing that saves us from the bureaucracy is its inefficiency.*"[1]

—Eugene McCarthy

Throughout the last decade, the government has waged war on federally funded improper payments,[2] which have recently ballooned to over $100 billion annually.[3] In 2011, the government rolled out a powerful weapon to help agencies combat their improper payments: the "Do Not Pay" Initiative ("Do Not Pay").[4] Do Not Pay "allows agencies to check various data

1. Eugene McCarthy, *On the Record*, TIME, Feb. 12, 1979, at 67.

2. *See infra* Part II.A (discussing in-depth what improper payments are in the context of government spending).

3. *See* Danny Werfel & Jeffrey C. Steinhoff, *Are You Combat Ready to Win the War Against Improper Payments?*, 63 J. GOV'T FIN. MGMT. 18, 19 n.4 (2014) ("Actual reported improper payment amounts—$105 billion for 2009; $121 billion for 2010; $115 billion for 2011; $108 billion for 2012; and $106 billion for 2013."); *see also infra* note 59 and accompanying text.

4. *See infra* Part II.B (discussing Do Not Pay, the government's solution to fighting improper payments).

sources for pre-award, pre-payment eligibility verification, at the time of payment and any time in the payment lifecycle."[5] In essence, Do Not Pay serves as a one-stop shop for government and private sector payee data, allowing government agencies to automate their payee eligibility investigations through computer matching and data analytics.[6]

While Do Not Pay has been an effective tool in combating improper payments,[7] automated investigation through computer matching raises individual privacy concerns.[8] In *The Digital Person*, Professor Daniel Solove[9] conceptualizes such concerns as a "Kafkaesque danger" after Franz Kafka's dystopian novel, *The Trial*.[10] Kafkaesque dangers involve data aggregation and automated investigation in a detached, bureaucratic governmental setting.[11] Computer matching has raised the specter of Kafkaesque dangers at least since the 1980s when Congress amended the Privacy Act of 1974 ("Privacy Act") to curtail government computer matching programs involving personal information.[12]

---

5. *What Can the Do Not Pay Business Center Do for Your Agency?*, DO NOT PAY, http://donotpay.treas.gov/index.htm (last updated Jan. 26, 2017, 8:25 AM).

6. *See infra* Part II.C. The Privacy Act defines computer matching in part as:

> [A]ny computerized comparison of . . . two or more automated systems of records or a system of records with non-Federal records for the purpose of—(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or (II) recouping payments or delinquent debts under such Federal benefit programs . . . .

Privacy Act of 1974, 5 U.S.C. § 552a(a)(8)(A) (2012).

7. *See infra* Part II.C (discussing the results of Do Not Pay).

8. *See infra* Part II.C (discussing the legal challenges to automated investigation activities posed by the Privacy Act).

9. Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. *Daniel Justin Solove*, GEO. WASH. L. SCH., https://www.law.gwu.edu/daniel-justin-solove (last visited Mar. 12, 2017). Professor Solove is internationally known for his expertise in privacy law and has published extensively on the subject. *See id.*

10. DANIEL J. SOLOVE, THE DIGITAL PERSON 177, 181 (2004). Kafka's novel involves "the surreal nightmare of a person who is unexpectedly informed that he is under arrest but given no reason why." *Id.* at 8. The individual "desperately attempts to find out why the Court is interested in his life, but his quest is hopeless—the Court is too clandestine and labyrinthine to be fully understood." *Id.* at 9. *See generally* FRANZ KAFKA, THE TRIAL (Ritchie Robertson ed., Mike Mitchell trans., 2009). The term "Kafkaesque" alludes to bureaucracy and refers to something "marked by a senseless, disorienting, often menacing complexity." *Kafkaesque*, DICTIONARY.COM, http://dictionary.reference.com/browse/kafkaesque (last visited Mar. 12, 2017).

11. SOLOVE, *supra* note 10, at 177–81.

12. *Id.* at 181, 257 n.72. The Privacy Act "governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies." *Privacy Act of 1974*, U.S. DEP'T JUST., http://www.justice.gov/opcl/privacy-act-1974 (last updated July 17, 2015). The Privacy Act was amended in 1988 in direct response to "significant concerns" over the government's computer matching programs. SOLOVE, *supra* note 10, at 181; *see also generally* Kenneth James Langan, *Computer Matching Programs: A Threat to*

Fast-forward to 2012 and the Privacy Act amendment largely prevented government agencies from using the personal information contained in Do Not Pay's databases to conduct computer matching activities.[13] This was problematic because computer matching with personal information derives the very best, most conclusive improper payment results.[14] The only way an agency could utilize Do Not Pay's personal information was to acquire "permission" from the government agency that supplied the personal information to Do Not Pay in the first place. Under the Privacy Act, such permission comes in the form of a computer matching agreement ("CMA"),[15] a difficult, administratively burdensome process for an agency to complete.[16] Do Not Pay consists of several databases subject to Privacy Act protection—agencies therefore needed to complete at least one, if not more, CMAs before matching on Do Not Pay's restricted databases.[17] This administrative burden was simply too much for many agencies to bear.[18] To alleviate this problem, legislators changed how the Privacy Act applies to Do Not Pay by passing the Improper Payments Elimination and Recovery Improvement Act of 2012 ("IPERIA").[19]

IPERIA contains a key language change to the Privacy Act relating to the CMA requirements for Do Not Pay.[20] The Office of Management and

---

Privacy?, 15 COLUM. J.L. & SOC. PROBS. 143 (1979). In the Privacy Act, personal information means "the name of the individual or . . . some identifying number, symbol, or other identifying particular assigned to the individual." Privacy Act of 1974, 5 U.S.C. § 552a(a)(5) (2012). Such personal information may include: name, date of birth, social security number, taxpayer identification number, debtor delinquency information, and incarceration information. *See* MARCELA SOUAYA, U.S. DEP'T OF THE TREASURY, GETTING RESULTS: HOW PRIVACY COMPLIANCE CAN IMPROVE YOUR AGENCIES' MATCHING POTENTIAL AND REDUCE IMPROPER PAYMENTS 6 (2014), https://www.fiscal.treasury.gov/fstraining/events/GettingResultsHowPrivacyCompliancecanImproveyourAgenciesMatchingProgram.pdf.

13. *See infra* Part II.C.

14. *See infra* note 77 and accompanying text (discussing the fact that matching on restricted data sources—data sources containing personal information—creates better results).

15. *See infra* Part II.C.

16. *See* 5 U.S.C. § 552a(o)(1) (enumerating requirements (A)–(K) to establish a CMA). Requirements (A)–(K) task agencies with developing extensive new procedures for, among other things, information verification, retention, destruction, security and notice to individuals. *See id.* Agencies must also justify why they want to engage in a matching program, the anticipated results of the program, and their legal authority to establish a program in the first place. *See id.*

17. *See infra* Part II.C.

18. *See infra* note 77 and accompanying text (discussing that agencies should weigh the workload against the benefits of establishing a CMA).

19. Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390, 2395 (2013).

20. *See id.* § 5(e)(2)(D) ("For purposes of this paragraph, section 552a(o)(1) of title 5, United States Code, shall be applied by substituting 'between the source agency and the recipient agency or non-Federal agency *or an agreement governing multiple agencies*' for 'between the source agency and the recipient agency or non-Federal agency' . . . ." (emphasis added)).

Budget ("OMB") issued guidance M-13-20 interpreting this change to allow qualifying agencies to collectively satisfy the requirements of a CMA with Do Not Pay through one "multilateral CMA."[21] With a multilateral CMA, qualifying agencies may gain access to the personal information in Do Not Pay—and thus utilize its full computer matching capabilities—at only a fraction of the work it took prior to IPERIA.[22] Together, Do Not Pay and IPERIA ushered in a new era of administrative efficiency in the CMA process.

This Note argues that IPERIA's change to the Privacy Act raises important policy concerns for individual privacy and that the OMB should implement changes to address these concerns. Part II of this Note traces the recent history of the government's fight against improper payments, leading up to the necessity and passing of IPERIA. Part III determines that IPERIA's change to the Privacy Act raises Kafkaesque dangers from Do Not Pay, and then concludes that on balance, OMB's M-13-20 guidance fails to mitigate the risks these dangers pose to individual privacy. Finally, Part IV proposes four key changes OMB can make to bolster individual privacy protections with the advent of the multilateral CMA. These changes call for greater oversight and effectiveness from the agency data integrity boards and new clarity in the qualifying test for the multilateral CMA option.

II. IMPROPER PAYMENTS AND THE DO NOT PAY INITIATIVE

A. *WHAT ARE IMPROPER PAYMENTS?*

In 2002, Congress passed the Improper Payments Information Act ("IPIA").[23] This Act requires government agencies to identify, estimate, and report on the scale of their annual improper payments.[24] It defined an improper payment as "any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other

21. *See* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB MEMORANDUM NO. M-13-20, PROTECTING PRIVACY WHILE REDUCING IMPROPER PAYMENTS WITH THE DO NOT PAY INITIATIVE 14 (Aug. 16, 2013) [hereinafter OMB MEMORANDUM M-13-20]. "The term 'multilateral computer matching agreement' (multilateral CMA) means a computer matching agreement that involves more than two agencies. For the purposes of a Do Not Pay matching program involving Treasury's Working System, a multilateral computer matching agreement involves Treasury and more than one payment-issuing agency." *Id.* at 5 (footnote omitted).

22. *See id.* at 14 (discussing, for example, the ability for agencies to "designate a single agency to report the CMA to OMB and Congress and publish the notice in the Federal Register on behalf of the other agencies"); *see also infra* Part III.A (discussing agencies cooperatively entering into one multilateral CMA with Do Not Pay to gain access to Do Not Pay's restricted content). In short, the multilateral CMA allows several agencies to join together to complete one CMA, rather than each agency individually completing a CMA with Do Not Pay.

23. Improper Payments Information Act of 2002, Pub. L. No. 107-300, 116 Stat. 2350.

24. *Id.* § 2.

legally applicable requirements."[25] Just two pages in length, this Act would serve as the foundation for the government's 21st-century fight against fraud, waste, and abuse in federally funded payments.[26]

With new reporting in place, the scale of improper payments came into focus. By fiscal year 2009, reporting found the government was making at least $100 billion in improper payments annually[27]—roughly the combined 2016 net worth of Mark Zuckerberg and Warren Buffett.[28] But this number deserves some unpacking, as not all improper payments represent a loss to the government.[29] A payment may be improper because it is: (1) an incorrect amount paid to eligible recipients; (2) a payment made to ineligible recipients; (3) a payment for goods or services not received; (4) a duplicate payment; or (5) a payment for which insufficient or no documentation was found.[30] Thus, an improper payment may be due to some unintentional error, such as a lack of supporting documentation or a data entry mistake, rather than an intentional misuse of funds.[31]

On the other hand, an improper payment may be the result of fraud, waste, or abuse. In 2009, the Government Accountability Office found that improper payments may result from such illicit activities as: improper unemployment payments, bribery, kickbacks, bid rigging, over-billing of labor and materials, improperly paid tax refunds, unemployment payments, tax return filing fraud, overpayments to vendors or contractors, tax credits,

---

25. *Id.* § 2(d)(2). The Act also defines an improper payment as "any payment to an ineligible recipient, any payment for an ineligible service, any duplicate payment, payments for services not received, and any payment that does not account for credit for applicable discounts." *Id.*

26. *See generally id.*

27. OFFICE OF INSPECTOR GEN., DEP'T OF THE TREASURY, OIG-15-006, AUDIT REPORT: FISCAL SERVICE SUCCESSFULLY ESTABLISHED THE DO NOT PAY BUSINESS CENTER BUT CHALLENGES REMAIN 3 (2014) [hereinafter OIG AUDIT REPORT OIG-15-006].

28. Keren Blankfeld, *Forbes Billionaires: Full List of the 500 Richest People in the World 2016*, FORBES (Mar. 1, 2016, 9:25 AM), https://www.forbes.com/sites/kerenblankfeld/2016/03/01/forbes-billionaires-full-list-of-the-500-richest-people-in-the-world-2016.

29. *Frequently Asked Questions*, PAYMENTACCURACY.GOV, https://paymentaccuracy.gov/faq (last visited Mar. 12, 2017) (noting within the subheading "What is an Improper Payment?" that "not all improper payments represent a loss to the government").

30. PAYMENTACCURACY.GOV, https://paymentaccuracy.gov (last visited Mar. 12, 2017). Within these four causes of improper payments, there have traditionally been three broad categories of improper payment errors: (1) documentation and administrative errors; (2) authentication and medical necessity errors; and (3) verification errors. *Frequently Asked Questions*, *supra* note 29 (under the subheading "What causes Improper Payments?"). However, in 2014 OMB expanded these three categories to 13 to create "a more meaningful and useful way to break out root cases [of improper payments] for each agency." *Id.* Agency reporting on these new categories was first required by OMB in fiscal year 2015. *Id.* The fiscal year 2015 breakout included the following root causes of improper payments: (1) "Program Design or Structural Issue"; (2) "Inability to Authenticate Eligibility"; (3) "Failure to Verify Data"; (4) "Administrative or Process Errors"; (5) "Medical Necessity"; (6) "Insufficient Documentation to Determine"; and (7) "Other Reason." *Id.*

31. *Frequently Asked Questions*, *supra* note 29 (noting within the subheading "What causes Improper Payments?" that improper payments may be caused by "a lack of supporting document necessary to verify the accuracy of a payment" or "incorrect data entry").

Medicare/Medicaid spending, and more.[32] Regardless of the cause, "improper payments degrade the integrity of government programs and compromise citizens' trust in government."[33]

In 2009, Barack Obama, a president far more publicly committed to government transparency than recent administrations, took office.[34] The Obama Administration made significant strides in providing transparency into government payment information. For example, the Obama Administration established several government websites dedicated to providing robust, timely, and accurate information on government payment systems, processes, and success rates.[35] The Obama Administration also noticed the high improper payment error rate and directed additional government resources to begin addressing the problem.[36]

B. THE GOVERNMENT ESTABLISHES THE DO NOT PAY INITIATIVE

A Presidential Memorandum calling for "Enhanced Payment Accuracy Through a Do Not Pay List" established the Do Not Pay Initiative on June 18, 2010.[37] Facially, the Memorandum presented a cognizable idea: make a list and check it twice before issuing a federally funded payment.[38] However,

---

32. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-628T, IMPROPER PAYMENTS: PROGRESS MADE BUT CHALLENGES REMAIN IN ESTIMATING AND REDUCING IMPROPER PAYMENTS 7–13 (2009).

33. *Frequently Asked Questions*, *supra* note 29.

34. *See* Clare Birchall, *Introduction to 'Secrecy and Transparency:' The Politics of Opacity and Openness*, 28 THEORY, CULTURE & SOC'Y 7, 11 (2011) (discussing President Obama setting in motion several open government initiatives and "position[ing] his administration on the side of openness from the beginning"); *see also* Memorandum on Transparency and Open Government, 2009 DAILY COMP. PRES. DOC. 10 (Jan. 26, 2009) (President Obama calling upon his administration "to creat[e] an unprecedented level of openness in Government").

35. *See, e.g.*, PAYMENTACCURACY.GOV, *supra* note 30; TRANSPARENCY.TREASURY.GOV, https://transparency.treasury.gov (last visited Mar. 12, 2017); RECOVERY.GOV, http://www.recovery.gov/Pages/default.aspx [https://web.archive.org/web/20160327000815/http://www.recovery.gov/Pages/default.aspx]; USASPENDING.GOV, https://www.usaspending.gov/Pages/Default.aspx (last visited Mar. 12, 2017).

36. Exec. Order No. 13,520, 74 Fed. Reg. 62,201 (Nov. 20, 2009).

37. Memorandum on Enhancing Payment Accuracy Through a "Do Not Pay List," 75 Fed. Reg. 35,953 (June 18, 2010). A timeline of events leading up to the Memorandum can be found here: Press Release, The White House Office of the Press Sec'y, President Obama to Sign Improper Payments Elimination and Recovery Act (July 22, 2010), https://www.whitehouse.gov/the-press-office/president-obama-sign-improper-payments-elimination-and-recovery-act [http://web.archive.org/web/20100723182036/http://www.whitehouse.gov/the-press-office/president-obama-sign-improper-payments-elimination-and-recovery-act].

38. The practice of checking a list before awarding a contract or grant is common, if not required, in many of the government's dealings with private entities. *See System for Award Management User Guide*, GEN. SERVICES ADMIN.: SYS. FOR AWARD MGMT., https://www.sam.gov/sam/SAM_Guide/SAM_User_Guide.htm (last visited Mar. 13, 2017) (consolidating four awardee verification registry systems: Central Contractor Registry, Federal Agency

the substance of the Memorandum made clear that President Obama intended something far more dynamic than a simple "list" of whom the government should or should not pay.

In his Memorandum, President Obama directed government agencies to adjust their pre-payment and pre-award procedures by reviewing payee eligibility against five government databases, designated as the "Do Not Pay List."[39] The "Do Not Pay List" databases include: Social Security Administration's Death Master File,[40] General Service Administration's ("GSA") Excluded Parties List System ("Excluded Parties"),[41] the Department of the Treasury's Debt Check Database,[42] the Department of Housing and Urban Development's Credit Alert System,[43] and the Department of Health and Human Services' ("HHS") List of Excluded Individuals/Entities ("Excluded Individuals").[44] The Memorandum then

---

Registration, Online Representations and Certifications Application, and General Services Administration's Excluded Parties List System).

39. Memorandum on Enhancing Payment Accuracy Through a "Do Not Pay List," *supra* note 37, at 35,953.

40. The Death Master File is a compilation of "death reports from many sources, including family members, funeral homes, financial institutions, postal authorities, States and other Federal agencies." *Requesting The Full Death Master File (DMF)*, SOC. SECURITY ADMIN., https://www.ssa.gov/dataexchange/request_dmf.html (last visited Mar. 15, 2017).

41. The Excluded Parties List is a list of businesses or individuals that a government agency has excluded (i.e. suspended or debarred) from "receiving contracts or assistance for various reasons, such as a conviction of or indictment for criminal or civil offense or a serious failure to perform to the terms of a contract." U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-174, EXCLUDED PARTIES LIST SYSTEM: SUSPENDED AND DEBARRED BUSINESSES AND INDIVIDUALS IMPROPERLY RECEIVE FEDERAL FUNDS 1 (2009) (footnote omitted). The Excluded Parties List has been consolidated into "SAM exclusion records." *See supra* note 38 (discussing the System of Award Management program consolidating four awardee verification systems including the Excluded Parties List).

42. Debt Check "allow[s] agencies and outside lenders to obtain information regarding whether applicants for federal loans, loan insurance or loan guarantees owe delinquent child support or delinquent non-tax debt to the federal government." Office of Legislative & Pub. Affairs, U.S. Dep't of the Treasury, *Fact Sheets: Debt Check*, BUREAU FISCAL SERV., http://fms.treas.gov/news/factsheets/debtcheck.html (last visited Mar. 15, 2017).

43. The Credit Alert System is a "database of defaulted Federal debtors, and enables processors of applications for Federal credit benefit to identify individuals who are in default or have had claims paid on direct or guaranteed Federal loans, or are delinquent or other debts owed to Federal agencies." *CAIVRS—Credit Alert Verification Reporting System*, U.S. DEP'T HOUSING & URBAN DEV., http://portal.hud.gov/hudportal/HUD?src=/program_offices/housing/sfh/caivrs (last visited Mar. 15, 2017).

44. The Excluded Individuals list is a list of "individuals and entities [excluded] from Federally funded health care programs pursuant to sections 1128 and 1156 of the Social Security Act." *Background Information*, U.S. DEP'T HEALTH & HUM. SERVS.: OFF. INSPECTOR GEN., http://oig.hhs.gov/exclusions/background.asp (last visited Mar. 15, 2017). Individuals and entities on this list participated in fraud, criminal, or other illegal activities. *Id.* For a concise listing of all current Do Not Pay databases, including databases beyond those in the "Do Not Pay List," see *Data Sources*, DO NOT PAY, http://donotpay.treas.gov/Resources.htm (last updated Jan. 26, 2017, 2:48 PM).

called for the Director of the OMB to develop a plan to integrate these five databases into a "single entry point" for government agencies.[45]

Thus, the true design of President Obama's "Do Not Pay List" was a government system that combines various government data sources into one repository of payee eligibility information, which is then made available to agencies to help identify and prevent improper payments.[46] A government system that identifies improper payments before it issues them easily garnered bipartisan support[47] as Congress shortly followed President Obama's Memorandum by passing the Improper Payments Elimination and Recovery Act of 2010, which "incorporated most of the requirements of the June 18, 2010 Presidential Memorandum into law."[48]

While the idea of a "Do Not Pay List" was appealing, developing and implementing such a program presented a daunting technological task.[49] To effectuate the program, OMB directed the Bureau of the Fiscal Service to begin developing the "Do Not Pay List."[50] The Fiscal Service, in turn, leveraged its fiscal agent relationship with the Federal Reserve[51] to provide for the various needs of the program such as technology development, user support, and customer service.[52] Fiscal Service's decision to use the Federal

45. Memorandum on Enhancing Payment Accuracy Through a "Do Not Pay List," *supra* note 37, at 35,953.

46. *Id.*

47. *See S. 1508 (111th): Improper Payments Elimination and Recovery Act of 2010*, GOVTRACK, https://www.govtrack.us/congress/votes/111-2010/h442 (last visited Mar. 15, 2017) (noting the final vote tally in the House was 414 yea, 0 nay, 18 not voting). In the Senate, "[t]he vote was by Unanimous Consent so no record of individual votes was made." *See id.*

48. OIG AUDIT REPORT OIG-15-006, *supra* note 27, at 5; *see also* Press Release, The White House Office of the Press Sec'y, *supra* note 37.

49. *See Data Integration*, DATA INTEGRATION INFO, http://www.dataintegration.info/data-integration (last visited Mar. 15, 2017) (discussing the challenges of integrating data from disparate and often incompatible sources). Interestingly, President Obama's Memorandum references the Federal Awardee Performance and Integrity Information System ("FAPIIS") as an initial integration effort of the "Do Not Pay List" databases. *See generally* Memorandum on Enhancing Payment Accuracy Through a "Do Not Pay List," *supra* note 37. As it would turn out, FAPIIS has had no direct interaction with the Do Not Pay Initiative and featured no part in the initial development of the program. *Compare Help*, FED. AWARDEE PERFORMANCE & INTEGRITY INFO. SYS., https://www.fapiis.gov/fapiis/help.action (last visited Mar. 15, 2017), *with Data Sources*, *supra* note 44. Thus, the Federal Reserve effectively started from scratch in developing this complex system.

50. OIG AUDIT REPORT OIG-15-006, *supra* note 27, at 2.

51. *See* Paula V. Hillery & Stephen E. Thompson, *The Federal Reserve Banks as Fiscal Agents and Depositories of the United States*, 2000 FED. RES. BULL. 251, 251 ("The Federal Reserve Act of 1913 provides that the Federal Reserve Banks will act as fiscal agents and depositories of the United States when required to do so by the Secretary of the Treasury. . . . The Reserve Banks' fiscal agency and depository services are related to their involvement in the broader payments system. . . . The Treasury and the Reserve Banks routinely modify, automate, or consolidate [payment] operations to achieve efficiencies and to reduce expenses over time.").

52. Kathleen O'Neill Paese, *Fiscal Agent for the U.S. Treasury*, FED. RES. BANK ST. LOUIS, https://www.stlouisfed.org/annual-report/2013/paese (last visited Mar. 15, 2017); *see also* OIG AUDIT REPORT OIG-15-006, *supra* note 27, at 1.

Reserve to develop the "Do Not Pay List" resulted in a dual benefit: Fiscal Service could leverage individual Reserve Bank strategic competencies while eliminating private sector profit margins.[53]

This partnership recast the "Do Not Pay List" as the "Do Not Pay Business Center," a multi-functional analytics tool and one-stop data shop for government agencies to verify payee eligibility.[54] By April 2012, the Do Not Pay Business Center was available for government agencies to use at no cost.[55] Elizabeth Owens, Sikich LLP, and Carol M. Jessup, Associate Professor of Accounting with the University of Illinois Springfield, summarize some of the benefits of Do Not Pay as follows:

> [Do Not Pay] helps prevent situations such as paying pension payments to a deceased person, paying a federal inmate or paying a contractor who has defrauded or attempted to defraud the government in the past. The user is able to look up a vendor to determine if he or she is excluded from receiving federal payments, ensure an individual receiving unemployment is still alive, determine if the vendor requires additional oversight due to past performance, and verify the accuracy of income.[56]

Reminiscent of President Obama's Memorandum, Do Not Pay's mission is to "[p]rotect the integrity of the government's payment process by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner while safeguarding the privacy of individuals."[57] Ironically, "safeguarding the privacy of individuals" would soon become one of the most significant administrative challenges to Do Not Pay's success.

C. DO NOT PAY INITIATIVE RESULTS AND CHALLENGES

The year 2015 marked the five-year anniversary of the Do Not Pay Initiative. By several accounts, Do Not Pay has become an important tool in

---

53. *See* OIG AUDIT REPORT OIG-15-006, *supra* note 27, at 8 ("Fiscal Service selected the Federal Reserve Bank of Kansas City to operate the Do Not Pay program and the Federal Reserve Bank of St. Louis to provide related support services. These Federal Reserve Banks were selected based on their expertise in Fiscal Service's payment processes, experience with other bureau initiatives, information technology capabilities, geographic locations near Fiscal Service payment processing centers, and overall costs."). As a former Senior Analyst at the Federal Reserve Bank of Kansas City, I can personally attest to the high degree of professionalism and dedication these individuals have to their work.

54. *What Can the Do Not Pay Business Center Do for Your Agency?*, *supra* note 5. The Do Not Pay Business Center, part of the Do Not Pay Initiative, includes a web-based portal (which effectuates the "Do Not Pay List" in President Obama's June 10 Memorandum), a data analytics service, and an agency support center. *Id.*

55. *Id.*; Elizabeth Owens & Carol M. Jessup, *Federal Improper Payments: An Overview*, 63 J. GOV'T FIN. MGMT. 12, 14 (2014).

56. Owens & Jessup, *supra* note 55, at 14.

57. *What Can the Do Not Pay Business Center Do for Your Agency?*, *supra* note 5.

the government's effort to reduce improper payments.[58] During the period between fiscal year 2009 and 2013, the improper payment rate dropped 35%, representing a total improper payment avoidance of $93 billion.[59] Moreover, based on the success of the program, OMB issued a Memorandum in 2012 directing all agencies to use the Do Not Pay Business Center.[60] In 2014, the Brookings Institute listed Do Not Pay as one of its "Top 10 Tech Innovations That Will Transform Society and Governance."[61] In 2015, Congress passed the Federal Improper Payments Coordination Act, which expanded the reach of Do Not Pay to states and the judiciary, representing unprecedented government coverage for the program.[62]

But Do Not Pay's success was not a guarantee. In its first year of operation, the Privacy Act, a law passed at the height of the Watergate scandal, presented a substantial roadblock to agency use of Do Not Pay.[63]

---

58. Danny Werfel, *Do Not Pay Solution Open for Business*, WHITE HOUSE: PRESIDENT BARACK OBAMA (Apr. 12, 2012, 12:32 PM), https://obamawhitehouse.archives.gov/blog/2012/04/12/do-not-pay-solution-open-business.

59. Werfel & Steinhoff, *supra* note 3, at 19 & n.1 ("Actual reported improper payment rates—5.42 percent for 2009 (base year); 5.29 percent for 2010; 4.69 percent for 2011; 4.35 percent for 2012; and 3.53 percent for 2013."). Interestingly, fiscal year 2016 (most recently available data) saw an uptick in actual reported improper payment rates to 4.67%. *See Improper Payment Rates Across the Federal Government*, PAYMENTACCURACY.GOV, https://paymentaccuracy.gov/improper-payment-rates-across-the-federal-government (last visited Mar. 15, 2017). But increased error rates in Medicaid were likely the "main culprit." *See* Jared Serbu, *Government Made $137 Billion in Improper Payments in 2015, Largest Figure on Record*, FED. NEWS RADIO: MGMT. (Feb. 26, 2016, 5:36 AM), http://federalnewsradio.com/management/2016/02/government-made-137-billion-improper-payments-2015-largest-figure-record. This matters, for purposes of this Note, because Medicare and Medicaid improper payments are addressed through the Centers for Medicare & Medicaid Services Center for Program Integrity rather than Do Not Pay. *See Center for Program Integrity*, AM. HEALTH CARE ASS'N, https://www.ahcancal.org/facility_operations/integrity/Pages/Center-for-Program-Integrity.aspx (last visited Mar. 15, 2017) ("CMS' Center for Program Integrity (CPI) mission is to protect the Medicare & Medicaid Trust funds against losses from fraud and abuse and other improper payments, and to improve the integrity of the health care system.").

60. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB M-12-11, REDUCING IMPROPER PAYMENTS THROUGH THE "DO NOT PAY LIST" (2012) [hereinafter OMB MEMORANDUM M-12-11]. *But see Frequently Asked Questions*, DO NOT PAY, http://donotpay.treas.gov/FAQs.htm (last visited Mar. 15, 2017) (stating that agencies are only "strongly encourage[d]" to use Do Not Pay's services).

61. Joshua Bleiberg & Darrell M. West, *TechTank's Top 10 Tech Innovations That Will Transform Society and Governance*, BROOKINGS (Dec. 22, 2014), http://www.brookings.edu/blogs/techtank/posts/2014/12/22-techtank-top-innovations-2014.

62. *See generally* Federal Improper Payments Coordination Act of 2015, Pub. L. No. 114-109, 129 Stat. 2225. The Federal Improper Payments Coordination Act of 2015 represents the third law passed in just five years pertaining directly to Do Not Pay and improper payments. With strong bipartisan support, the government has been able to aggressively broaden the scope and capabilities of the Do Not Pay program with little pushback. This should give one pause and invite careful discussion about the policy concerns that exist with an ever-expanding system that conducts continuous automated investigation activities into the lives and affairs of United States persons. *See infra* Part III.B.

63. *See* Dept. of Homeland Sec. Office for Civil Rights & Civil Liberties & Dept. of Homeland Sec. Privacy Office, *Privacy Act of 1974, 5 U.S.C. § 552a*, U.S. DEP'T JUST.: JUST. INFO. SHARING (Aug.

"The Privacy Act . . . governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."[64] A "'system of records' . . . [is] a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[65]

A 1988 amendment to the Privacy Act requires that "no record which is contained in a system of records may be disclosed to a recipient agency or non-[f]ederal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-[f]ederal agency."[66] This means that, if an agency wants to share its system of record data for any computerized matching activities, it must establish a Computer Matching Agreement[67] with the recipient agency or non-federal agency, unless it is exempted from Privacy Act requirements.[68] Additionally, the respective agency's data integrity board—a board comprised of senior agency personnel charged with overseeing and coordinating Privacy Act requirements for computer matching programs—must review and approve any new computer matching program.[69]

The Privacy Act significantly affected Do Not Pay, given that four out of the five databases in the "Do Not Pay List" were designated as a system of record.[70] In practice, before any recipient agency could match its payee data

---

16, 2013), https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279 (discussing how the Privacy Act was passed at the height of the Watergate Scandal, and how "Congress was concerned with curbing the illegal surveillance and investigation of individuals . . . [as well as] potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier").

64. *Privacy Act of 1974*, *supra* note 12.

65. Privacy Act of 1974, 5 U.S.C. § 552a(a)(5) (2012).

66. *Id.* § 552a(o)(1).

67. *See id.*

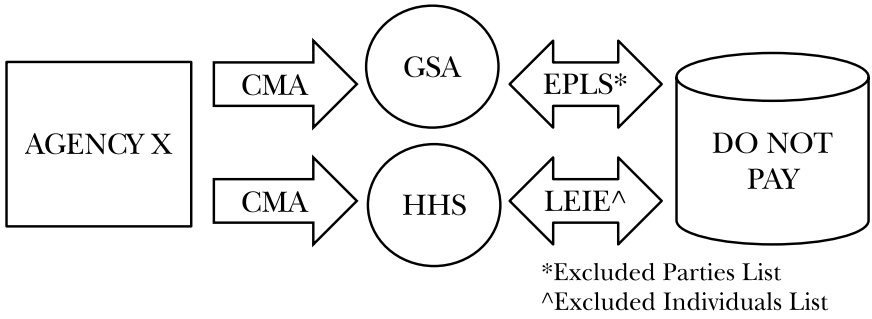
68. *See* 28 C.F.R. § 16.70–16.136 (2016) (listing systems of records that are exempted from certain Privacy Act requirements); *see also* 5 U.S.C. § 552a(j)–(k) (detailing system of record exemption requirements).

69. *See* 5 U.S.C. § 552a(u) (describing Data Integrity Boards); OMB MEMORANDUM M-13-20, *supra* note 21, at 4 (defining "Data Integrity Board").

70. The only database in the original "Do Not Pay List" that is not subject to system of record requirements is the Death Master File. This is because Do Not Pay currently uses the "public" version of the Death Master File. *See Data Sources*, *supra* note 44 (providing a list of currently available data sources and showing the Death Master File as a "public" source). The "public" version of the Death Master File contains no restricted personal information, and is therefore not subject to CMA requirements. *See infra* note 79 and accompanying text. This appears to be set for change, however, with the passing of the Federal Improper Payments Coordination Act of 2015, which grants Do Not Pay access to "[t]he death records maintained by the Commissioner of Social Security" in lieu of "[t]he Death Master File of the Social Security Administration." Federal Improper Payments Coordination Act of 2015, Pub. L. No. 114-109, § 3(1)(A), 129 Stat. 2225, 2226; *see also* Improper Payments Elimination and

against personal information—considered "restricted content"—within one of the system of record-designated databases in the "Do Not Pay List," it needed to establish a CMA with the agency (or agencies) that supply the "Do Not Pay List" databases to Do Not Pay.[71] For example, if Agency X wanted to match its payee data against restricted content in the Excluded Parties List and the Excluded Individuals List, Agency X needed to establish a CMA with, and receive data integrity board approval from, GSA and HHS respectively (Figure 1).[72]

Figure 1: Do Not Pay CMA Requirements Before IPERIA



Establishing a CMA is a difficult process; the Privacy Act enumerates 11 complex specifications that an agency must meet before a CMA is approved.[73] Moreover, the Privacy Act's CMA requirements have a broad reach, as there are hundreds of systems of records spanning numerous agencies.[74] The policy rationale for these extensive requirements is principally to protect personal information from capricious government computer matching. Yet for a program like Do Not Pay, the Privacy Act created a substantial administrative burden for agencies wishing to match their payee data against the personal information contained in Do Not Pay.[75]

Recovery Improvement Act of 2012, Pub. L. No. 112-248, § 5(a)(2)(A), 126 Stat. 2390, 2393 (2013). Presumably, the Federal Improper Payments Coordination Act of 2015 will allow Do Not Pay to access restricted death data.

71. *See* BUREAU OF THE FISCAL SERVICE, DO NOT PAY AGENCY IMPLEMENTATION GUIDE FOR TREASURY'S WORKING SYSTEM 52 (2017), https://donotpay.treas.gov/DNPAgencyImplementationGuidePublic.pdf [hereinafter DO NOT PAY AGENCY IMPLEMENTATION GUIDE] ("The original-source agency would be one of those agencies that have one of the IPERIA mandated databases, such as [the Excluded Parties list]. The payment-issuing agency is any agency that wants to match its files against one of the IPERIA mandated restricted databases."). IPERIA codified the "Do Not Pay List" databases into law. *See* Improper Payments Elimination and Recovery Improvement Act of 2012 § 5(b)(1).

72. *See* SOUAYA, *supra* note 12, at 8 (providing an "[e]xample of [system of record]'s impact").

73. *See* 5 U.S.C. § 552a(o)(1)(A)–(K).

74. *Privacy Act Systems of Records Notices*, SOC. SEC. ADMIN, https://www.ssa.gov/foia/bluebook/ (last visited Feb. 23, 2017).

75. *See generally* 5 U.S.C. § 552a.

New administrative burdens are rarely met with excitement, and agencies began looking for alternative ways to satisfy OMB's requirement to use Do Not Pay.[76] It was not long before agencies discovered the Privacy Act's CMA requirements could be circumvented through matching on the "public" versions of the "Do Not Pay List" databases.[77] Several of the "Do Not Pay List" databases are available in both "public" and "restricted" versions, with the public version containing no personal information.[78] Since the public versions contain no personal information, they do not trigger the Privacy Act requirements for a CMA.[79] The end result? Agencies could quickly "satisfy" their requirement to use Do Not Pay without having to go through the rigmarole of establishing CMAs.

While this approach ostensibly relieved agencies of the need to complete CMAs, it also created a problem: matching without the aid of personal information produced less conclusive results and more false positives (a false positive is a match that is later found to involve an eligible payee and a proper payment).[80] When an agency chooses to match against publicly available versions of a database, Do Not Pay must use only data that is available to the public (such as first and last names), rather than more conclusive data available only in the restricted version of a database, like

---

76. *See supra* note 60 and accompanying text (discussing the requirement to use Do Not Pay).

77. The Do Not Pay Agency Implementation Guide provides that agencies should "assess [their] data source matching requirements before onboarding" to "help determine appropriate data source versions (whether public, restricted, or both) and address legal or regulatory obstacles for accessing data sources." DO NOT PAY AGENCY IMPLEMENTATION GUIDE, *supra* note 71, at 13. The implementation guide warns agencies "that matching with public versions of data sources can limit the effectiveness of the matching results . . . [and that] [i]n most cases, to match on the restricted versions of files, [the agency] must establish CMAs." *Id.* at 13–14. Finally, the implementation guide cautions agencies to "assess the benefit of having a CMA in place against the workload to establish CMAs." *Id.* at 14. Presumably, the workload of establishing CMAs outweighed the perceived benefits for many agencies before the passing of IPERIA.

78. *See* SOUAYA, *supra* note 12, at 6 (comparing public and restricted content in Do Not Pay data sources); *see also Frequently Asked Questions*, *supra* note 60 ("Public data sources are those available to members of the public via websites or other non-restricted means. Restricted data sources are not available to the public and house data sources that are protected by the Privacy Act. Privacy Act protected systems are characterized by those records under the control of any agency from which information is retrieved by a unique identifier (e.g., name, symbol, identifying particular assigned to an individual).").

79. 5 U.S.C. § 552a(a)(5), (o)(1).

80. *See* DO NOT PAY AGENCY IMPLEMENTATION GUIDE, *supra* note 71, at 52 ("Completion of the CMA will allow you to perform electronic matches with key data sources while ensuring that you maintain the privacy rights of individuals. Matching to files that require CMAs is one step that you can undertake that can significantly decrease the number of false positives that can occur when matching with the corresponding 'public' version of the same basic data. This can be critical to a more-timely reduction in the number of improper payments that occur at your agency."); *see also* SOUAYA, *supra* note 12, at 8. "When you research a match and determine that it was actually an eligible payee as well as a proper payment, then you would consider that payment a 'false positive.'" DO NOT PAY AGENCY IMPLEMENTATION GUIDE, *supra* note 71, at 14.

social security or taxpayer identification numbers.[81] By taking this lightweight approach to matching (i.e. matching on less conclusive data), the value of Do Not Pay is eroded and more manual work is created for agency users.[82] Recognizing this as a threat to the long-term success of the program, Congress stepped in to change how the Privacy Act applies to Do Not Pay.[83]

III. IMPROPER PAYMENT ELIMINATION AND RECOVERY IMPROVEMENT ACT

A. THE PURPOSE OF IPERIA

U.S. Senator Tom Carper (D-DE) introduced the Improper Payment Elimination and Recovery Improvement Act in 2012 ("IPERIA").[84] A champion against improper payments, Senator Carper also introduced the Improper Payment Elimination and Recovery Act in 2010, and IPERIA represented the next crucial step in fighting improper payments.[85] The stated purpose of IPERIA is "[t]o intensify efforts to identify, prevent, and recover payment error, waste, fraud, and abuse within Federal spending."[86] While IPERIA contained several important changes to how the government fights improper payments, section 5 directly addresses the Do Not Pay Initiative.[87]

---

81. *See* DO NOT PAY AGENCY IMPLEMENTATION GUIDE, *supra* note 71, 13–14 ("Be aware that matching with public versions of data sources can limit the effectiveness of the matching results. This limitation is often due in part to matching by name only, rather than matching by name and Taxpayer Identification Number (TIN). This can cause a number of false-positive matches. In most cases, to match on the restricted versions of files, you must establish CMAs.").

82. *Id.*; *cf.* SOUAYA, *supra* note 12, at 7 (discussing the "Benefits of Matching Against Restricted Sources").

83. The House Report paints a more progressive picture of the situation, stating:

> To better address this [improper payment] problem, agencies must take advantage of new technologies and data sharing capabilities. H.R. 4053 brings improper payment detection and prevention into the 21st century by encouraging the use of technology to allow agencies to *easily share data* to achieve increased payment accuracy and accountability.

H.R. REP. NO. 112-698, at 7 (2012) (emphasis added).

84. Press Release, Senator Tom Carper, Senator Carper Continues Efforts to Cut Waste, Fraud, and Abuse in Government Spending (Mar. 17, 2015), http://www.carper.senate.gov/public/index.cfm/pressreleases?ID=eeff5999-aec4-4357-97fb-db4c7fccb42e. "Sen. Carper was joined by Sen. Collins (R-Maine) and former Sen. Scott Brown (R-NH)" in introducing IPERIA. *Id.*

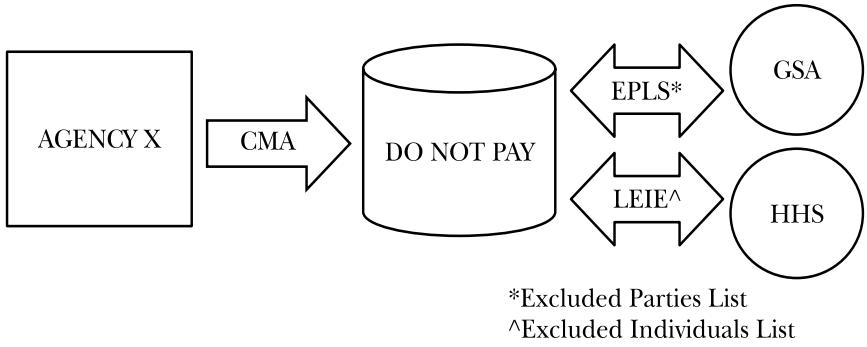
85. *Id.*

86. Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390, 2390 (2013).

87. *Id.* § 5. Section 5 officially codifies the Do Not Pay Initiative into law. *Id.* Section 5 also establishes a "Working System" which includes "investigation activities for fraud and systemic improper payments detection through analytic technologies." *Id.* § 5(d)(2)(C). This captures the full breadth of the Do Not Pay Business Center. *See What Can the Do Not Pay Business Center Do for Your Agency?*, *supra* note 5.

Section 5 of IPERIA granted Do Not Pay the authority to establish itself as a system of record, which it promptly did.[88] As a system of record, agencies wishing to match against restricted content in Do Not Pay now only need to establish one CMA with Do Not Pay, rather than multiple CMAs with source agencies.[89] Thus, where Agency X previously had to establish *two* CMAs (one with GSA and one with HHS) to match against restricted content in the Excluded Parties List and Excluded Individuals List (Figure 1), after IPERIA, Agency X need only establish *one* CMA with Do Not Pay (Figure 2).[90] Furthermore, if Agency X theoretically needed to match on all restricted databases in the "Do Not Pay List," Agency X would still only need to establish *one* CMA with Do Not Pay.[91] This change to the CMA process affords significant administrative efficiency for agencies and reduced the incentive to only use the public versions of the "Do Not Pay List" databases.

Figure 2: Do Not Pay CMA Requirements After IPERIA



88. Improper Payments Elimination and Recovery Improvement Act of 2012 § 5. The stated purpose of the Do Not Pay system of record is to "assist Federal agencies in verifying that individuals are eligible to receive Federal payments by allowing the Department of the Treasury/Bureau of the Fiscal Service to collect, maintain, analyze, and disclose records that will assist Federal agencies in identifying, preventing, and recovering payment error, waste, fraud, and abuse within Federal spending, as required by IPERIA." Privacy Act of 1974, as Amended; System of Records, 78 Fed. Reg. 73,923, 73,925 (Dec. 9, 2013).

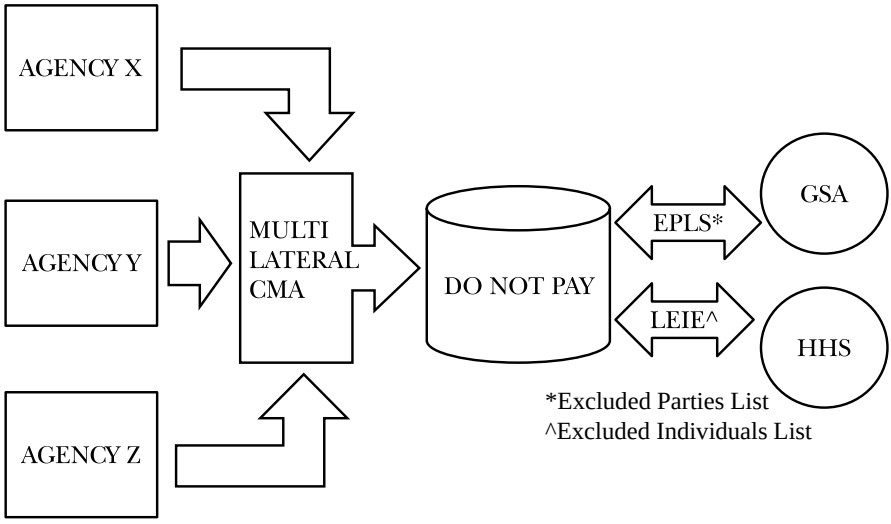
89. *See* SOUAYA, *supra* note 12, at 8 (providing an "[e]xample of [system of record]'s impact").

90. *Id*; *see infra* Figure 2.

91. SOUAYA, *supra* note 12, at 8. OMB's guidance M-13-20 requires Treasury (Do Not Pay) and original source agencies to enter Memorandums of Understanding ("MOUs") that describe how the Treasury may use the original source agency records in question, as well as provide rules for protecting, correcting, retaining, and destroying information and records. OMB MEMORANDUM M-13-20, *supra* note 21, at 6–7. Treasury is required to periodically review these MOUs to "determine whether the terms are sufficient." *Id.* at 6. In essence, the MOUs between Treasury and the original source agencies serve the purpose intended by the Privacy Act for CMAs, but are less administratively burdensome to complete.

But IPERIA does not stop there. Section 5 of IPERIA makes a key language change to how the Privacy Act applies to Do Not Pay.[92] Section 5 of IPERIA inserts additional language into section 552a(o)(1) to read: "between the source agency and the recipient agency or non-Federal agency *or an agreement governing multiple agencies*."[93] In August 2013, OMB issued guidance M-13-20 explaining that this language change allows agencies to establish a "multilateral computer matching agreement" ("multilateral CMA") with Do Not Pay.[94] A multilateral CMA is a computer matching agreement that involves the Treasury (i.e., Do Not Pay) and two or more agencies for the purpose of establishing a Do Not Pay matching program.[95] This change means that Agencies X, Y, and Z may collectively enter *one* multilateral CMA with Do Not Pay to gain access to Do Not Pay's restricted content (Figure 3).

Figure 3: The Multilateral CMA



However, the M-13-20 guidance requires each recipient agency to qualify for the multilateral CMA. To qualify, agencies must show that "the

92. Improper Payments Elimination and Recovery Improvement Act of 2012 § 5(e)(2)(D); *see also* OMB MEMORANDUM M-13-20, *supra* note 21, at 3 ("While IPERIA does not explicitly amend the definitions in the Privacy Act, it nonetheless changes how the Privacy Act applies for purposes of the DNP Initiative.").

93. Improper Payments Elimination and Recovery Improvement Act of 2012 § 5(e)(2)(D) (emphasis added).

94. OMB MEMORANDUM M-13-20, *supra* note 21, at 5.

95. *See supra* text accompanying note 21.

matching purpose and the specific data elements that will be matched are sufficiently similar across each of the agencies to allow all parties to satisfy the requirements in a single CMA that is clear to all relevant agencies and to the public."[96] Before Agencies X, Y, and Z can enter a multilateral CMA, they must qualify through the above test. If all three qualify, they can now enter one multilateral CMA together with Do Not Pay. On the surface, this test sounds reasonable yet it is not clear what "sufficiently similar" means in the context of specific agency data elements. This leaves the door open for interpretation and, possibly, abuse.[97]

Arguably, allowing Do Not Pay to become a system of record, and thus a single CMA point of contact for agencies, still protects individual privacy interests from capricious computer matching.[98] The multilateral CMA, however, is a groundbreaking development. The multilateral CMA significantly expedites OMB's directive for all agencies to use Do Not Pay[99] by allowing more agencies to onboard[100] in a shorter time and with greater ease.[101] It is unclear how many agencies may qualify for a multilateral CMA, but Congress's change to the Privacy Act indicates there is definite interest in such an option. This development raises some troubling policy concerns.

B. BALANCING ADMINISTRATIVE EFFICIENCY AND INDIVIDUAL PRIVACY INTERESTS

IPERIA's change to the Privacy Act and OMB's guidance establishing the multilateral CMA, collectively, beg the question as to whether IPERIA's new administrative efficiencies sacrifice too much privacy protection. On the one hand, IPERIA updates the Privacy Act by helping to reduce redundancies in the CMA process and aiding the government's fight against

96. OMB MEMORANDUM M-13-20, *supra* note 21, at 14.

97. *See infra* Part IV.D (discussing two ways to interpret sufficient similarity and advocating for a narrow interpretation as a way to safeguard individual privacy).

98. One assumes that all of the Privacy Act requirements to establish a CMA will still be satisfactorily met under this new arrangement, leaving the public at least no worse off than before IPERIA. One could even argue, perhaps, that because Do Not Pay is now positioned as a central point of contact for establishing CMAs, additional scrutiny and transparency will be demanded, allowing for greater sunshine into the CMA process.

99. *See generally* OMB MEMORANDUM M-12-11, *supra* note 60.

100. This Note uses the term "onboard" in the same context as the Do Not Pay Implementation Guide, generally meaning the "adoption, integration, and application of [Do Not Pay] as a solution to complement [an] agency's internal controls." DO NOT PAY AGENCY IMPLEMENTATION GUIDE, *supra* note 71, at 1. Onboarding generally refers to an agency completing "tasks, activities, and processes . . . in order to initiate and maximize use of [Do Not Pay]." *Id.*

101. In terms of ease, M-13-20 guidance provides "payment-issuing agencies may designate a single agency to report the CMA to OMB and Congress and publish the notice in the Federal Register on behalf of the other agencies." OMB MEMORANDUM M-13-20, *supra* note 21, at 14. Thus, M-13-20 not only reduces CMA redundancy, it cuts down on CMA reporting requirements.

improper payments.[102] On the other hand, IPERIA erodes the Privacy Act's CMA requirements—individual privacy protection—to allow more agencies to engage in advanced automated investigation activities through Do Not Pay's computer matching capabilities.[103] Further underscoring concerns over invasion of individual privacy, since Congress passed IPERIA, congressional and Treasury budget reports indicate Do Not Pay has spent tens of millions of dollars on improving its investigation technologies and acquiring more data.[104]

How one views IPERIA depends on the balance of interests between the new administrative efficiency of the multilateral CMA and individual privacy interests affected under the Privacy Act. In *Understanding Privacy*, Professor Solove writes: "To properly weigh privacy against conflicting interests, it is imperative that we have a complete understanding of the particular privacy problems involved in any given context. We must identify the privacy problems, examine the activities compromised by each, and recognize the nature of harms to these activities."[105] To achieve this complete understanding, this Note seeks to identify and weigh the privacy problems IPERIA raises to determine the appropriate balance between administrative efficiency and individual privacy as it relates to the multilateral CMA.

To conduct this analysis, Solove provides a helpful framework in *The Digital Person*.[106] Solove defines two paradigms of privacy based on twentieth century dystopian novels: an Orwellian paradigm and a Kafkaesque paradigm.[107] The characteristics of the Orwellian paradigm of privacy are government surveillance, secrecy, and attempts at societal control.[108] The Kafkaesque paradigm captures concerns of data aggregation and automated investigation in a detached and bureaucratic governmental setting.[109] In a government context, Solove recognizes that there are dangers from both

102. *See* Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390, 2390 (2013) (stating the purpose of the Act is "[t]o intensify efforts to identify, prevent, and recover payment error, waste, fraud, and abuse within Federal spending"). Intensifying efforts, for the purposes of this Note, includes the reinterpretation of a portion of the Privacy Act by substituting new language into section 552a(o)(1) to allow for multilateral CMAs. *See id.* § 5(e)(2)(D).

103. *See* SOLOVE, *supra* note 10, at 181 (discussing how the Privacy Act was amended in 1988 to require CMAs in direct response to "significant concerns" over the government's computer matching programs). These concerns were well documented by the time the Privacy Act was amended in 1988. *See generally* Langan, *supra* note 12.

104. *See* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, FISCAL YEAR 2015 ANALYTICAL PERSPECTIVES: BUDGET OF THE U.S. GOVERNMENT 124 (2014); BUREAU OF THE FISCAL SERV., FY 2015 CAPITAL INVESTMENT PLAN 14 (2015).

105. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 174 (2008).

106. *See generally* SOLOVE, *supra* note 10.

107. *See id.* at 7–9.

108. *See id.* at 7–8.

109. *See id.* at 9.

paradigms.[110] The Orwellian dangers include: (1) a slow creep towards totalitarianism; (2) a detrimental impact to democracy and self-determination; (3) interference with freedom of association; and (4) loss of anonymity.[111] The Kafkaesque dangers include: (1) leaks, lapses, and vulnerability; (2) automated investigations and profiling; and (3) changing purposes and uses.[112]

By analyzing IPERIA's changes to the CMA process for Do Not Pay through these two paradigms, the balance between administrative efficiency and individual privacy interests comes into focus. If Do Not Pay poses Orwellian dangers after IPERIA, it almost certainly represents an erosion of individual privacy interests.[113] On the other hand, if Do Not Pay falls within the Kafkaesque paradigm, the impact to individual privacy interests may be more attenuated.[114] In that case, this Note proposes that a risk analysis of the Kafkaesque dangers is necessary to better understand whether IPERIA actually creates valuable administrative efficiencies or facilitates a system that invades individual privacy through automated investigation activities.[115]

---

110. *See id.* at 175–85.

111. *See id.* at 175–77.

112. *See id.* at 177–85. Solove cites an additional Kafkaesque danger: overreacting in times of crisis. *See id.* at 182–84. This concern involves the government using its aggregated data to round up politically disfavored groups and individuals, such as during the Red Scare and World War Two. *See id.* at 182–83. IPERIA does not contain a discrete investigatory component, nor does it portend the government using Do Not Pay to politically silence political dissenters. This danger is therefore not seriously considered in this Note.

113. *Id.* at 175–77.

114. *Id.* at 177–84.

115. A risk analysis reduces the level of uncertainty posed by risks and allows one to focus on high priority risks. PROJECT MGMT. INST., A GUIDE TO THE PROJECT MANAGEMENT BODY OF KNOWLEDGE (PMBOK GUIDE) 328 (5th ed. 2013). A risk analysis involving a balancing of the interests is a familiar analytical tool in the context of privacy, particularly where Fourth Amendment search and seizure questions have arisen. *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("The critical question, therefore, is whether . . . we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement. This question must, in my view, be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."); Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting) (arguing that electronic surveillance changes the risk calculus substantially and that "[t]here is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy"). A comprehensive discussion of the nexus between the risks posed by new surveillance technology and data gathering techniques and the Court's Fourth Amendment privacy jurisprudence is beyond the scope of this Note. However, there is no shortage of material on this fascinating and rapidly evolving area of law. *See generally, e.g.*, Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809 (2014); Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579 (2014); Philip B. Heymann, *An Essay on Domestic Surveillance*, 8 J. NAT'L SECURITY L. & POL'Y 421 (2016); Harold Laidlaw, *Shouting Down the Well: Human Observation as a Necessary Condition of Privacy Breach, and Why Warrants Should Attach to*

1. IPERIA Falls Squarely Within the Kafkaesque Paradigm

It seems fairly clear that IPERIA's effect on Do Not Pay does not pose the sort of Orwellian dangers contemplated by Solove.[116] The defining theme amongst these dangers is some direct governmental interference with an individual's privacy.[117] Whether that interference is in the form of social control, freedom of speech, privacy in one's associations, or the ability to send and receive information freely, the Orwellian paradigm signifies the establishment and expansion of a surveillance state.[118] IPERIA's change to how agencies engage Do Not Pay through the CMA process does not readily invite these types of dangers.[119] For example, unlike government surveillance programs, IPERIA does not facilitate direct data aggregation from an unaware public.[120] Instead, IPERIA reduces the administrative burden for agencies seeking to engage Do Not Pay for restricted computer matching on data already collected through normal government agency processes.[121]

Under the Kafkaesque paradigm, on the other hand, Do Not Pay poses dangers that are immediately more apparent after IPERIA. By reducing the administrative burden of the CMA process, IPERIA facilitates agencies' access to restricted content in Do Not Pay, leading to more payee investigation activities.[122] More investigation means more payee personal information in the Do Not Pay system, making the Kafkaesque danger of leaks, lapses, and vulnerabilities (i.e., data breaches[123]) more perilous.[124]

Data Access, Not Data Gathering, N.Y.U. ANN. SURV. AM. L. 323 (2015); Emma Raviv, Note, *Homing In: Technology's Place in Fourth Amendment Jurisprudence*, 28 HARV. J.L. & TECH. 593 (2015).

116. *See supra* note 112 and accompanying text.

117. SOLOVE, *supra* note 10, at 175–77.

118. *See id.*

119. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390 (2013).

120. For an example of government surveillance, see Press Release, Director of National Intelligence, Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf. In contrast, IPERIA and Do Not Pay are not classified programs (though the information contained in Do Not Pay's databases is sensitive in nature) and information is readily available on each to the public. *See also* Craig Timberg et al., *WikiLeaks: The CIA is Using Popular TVs, Smartphones and Cars to Spy on Their Owners*, WASH. POST (Mar. 7, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/07/why-the-cia-is-using-your-tvs-smartphones-and-cars-for-spying.

121. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012; OMB MEMORANDUM M-12-11, *supra* note 60.

122. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012; OMB MEMORANDUM M-12-11, *supra* note 60.

123. A data breach is "[a]n unauthorized dissemination of information. It may be due to an attack on the network or outright theft of paper documents, portable disks, USB drives or laptops. Sensitive information can also be found in trash cans when reports are carelessly discarded." *Definition of: Data Breach*, PCMAG,

Data breaches can be incredibly costly and can cause irreparable harm for all parties involved.[125] If Do Not Pay experienced a data breach, that breach not only could expose personal information but could also cause the government to suffer significant reputational damage.[126] A string of high profile data breaches since 2000 demonstrate this danger all too well.[127]

Automated investigation is the principal Kafkaesque danger that results from computer matching under IPERIA.[128] With the use of computer matching, the government can automate the investigation of millions of people.[129] IPERIA makes the process significantly easier for qualifying agencies to enter a CMA with Do Not Pay because of IPERIA's multilateral CMA process.[130] That ease of process, in turn, will lead to more automated investigation of individual payees.[131] More automated investigation will likely result in the discovery of additional instances of fraud and improper payments—which is a good thing.[132] At the same time however, automated investigation is a fundamentally different way to investigate individuals.[133]

Typically, the government must have some factual basis to conduct individualized investigative activities.[134] With Do Not Pay however, an agency has the option of conducting one giant investigation of numerous payees through "batch matching."[135] Or, an agency may choose to constantly

---

http://www.pcmag.com/encyclopedia/term/61571/data-breach (last visited Mar. 15, 2017); *see also Data Breaches*, W. VA. ST. PRIVACY OFF., http://www.privacy.wv.gov/tips/Pages/DataBreaches.aspx (last visited Mar. 15, 2017).

124. *See* SOLOVE, *supra* note 10, at 179–80.

125. *See generally* PONEMON INST., THE AFTERMATH OF A MEGA DATA BREACH: CONSUMER SENTIMENT (2014), http://www.experian.com/assets/p/data-breach/experian-consumer-study-on-aftermath-of-a-data-breach.pdf.

126. In a recent high profile government data breach of the Office of Personal Management, the government suffered serious reputational damage and at least 20 million people were adversely affected. *See* Paul Coyer, *U.S. Government Data Breach Exemplifies China's Cyber Insecurities*, FORBES (July 19, 2015, 10:26 PM), http://www.forbes.com/sites/paulcoyer/2015/07/19/the-opm-data-breach-and-sino-american-competition/; Jim Sciutto, *OPM government data breach impacted 21.5 million*, CNN (July 10, 2015, 1:15 PM), http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million.

127. Lorenzo Ligato, *The 9 Biggest Data Breaches of All Time*, HUFFINGTON POST (Aug. 21, 2015, 11:20 AM), http://www.huffingtonpost.com/entry/biggest-worst-data-breaches-hacks_55d4b5a5e4b07addcb44fd9e.

128. SOLOVE, *supra* note 10, at 180.

129. *Id.*

130. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390 (2013); OMB MEMORANDUM M-12-11, *supra* note 60.

131. *See* DO NOT PAY AGENCY IMPLEMENTATION GUIDE, *supra* note 71, at 54 (stating that data sources that require a CMA can provide a more conclusive match).

132. *Id.*

133. SOLOVE, *supra* note 10, at 181.

134. *Id.*

135. *Frequently Asked Questions*, *supra* note 60 ("Batch Matching allows a comparison of an agency's pre-award and pre-payment file; DNP matches files to available approved data sources and returns the results in the portal.").

investigate its payees through a "continuous monitoring" service.[136] These computer matching services give agencies the ability to *constantly* investigate their payees. The Kafkaesque danger is that these automated investigations allow the government to deeply and continuously intrude into the lives and affairs of its people.[137] Automated investigation through computer matching does not discriminate, and unfortunately most people the system investigates are innocent.[138]

IPERIA also raises the Kafkaesque danger that Do Not Pay will engage in profiling[139] through its Data Analytics Services.[140] As Do Not Pay investigates more agency payee data, Do Not Pay will have more opportunities to develop comprehensive profiles as part of a larger effort to forecast fraudulent behaviors.[141] Borrowing from a private sector example of

---

136. *Id.* ("Continuous Monitoring allows an ongoing comparison of an agency's file against all data sources they are authorized to access.").

137. For a concise essay on why government intrusion into the lives and affairs of persons through surveillance and data mining matters, see generally Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007). Solove explores the "I have nothing to hide" argument, a typical retort in favor of government surveillance, and concludes that such an argument is a "singular and narrow way" to conceive of the "plurality of privacy problems" involved in governmental surveillance. *Id.* at 772. The Court has also expressed liberty concerns stemming from automated systems. *See* Herring v. United States, 555 U.S. 135, 155 (2009) (Ginsburg, J., dissenting) ("Inaccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty.").

138. *See* SOLOVE, *supra* note 10, at 181 (stating that "[c]omputer matches . . . investigate everyone, and most people who are investigated are innocent" (citing PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 90 (1995))).

139. *Id.* at 181 ("Profiles . . . use particular characteristics and patterns of activity to predict how people will behave in the future."); *see also* Mireille Hildebrandt, *Defining Profiling: A New Type of Knowledge?*, *in* PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINARY PERSPECTIVES 17, 17 (Mireille Hildebrandt & Serge Gutwirth eds., 2008) (providing a "simple working definition of profiling" as: "[t]he process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category"); Nancy J. King & Jay Forder, *Data Analytics and Consumer Profiling: Finding Appropriate Privacy Principles for Discovered Data*, 32 COMPUTER L. & SECURITY REV. 696, 698 (2016) (defining profiling as "'the process of discovering correlations between data in databases that can be used to identify and represent' a data subject and/or to place the data subject in a group or category" (quoting Bart W. Schermer, *The Limits of Privacy in Automated Profiling and Data Mining*, 27 COMPUTER L. & SECURITY REV. 45, 45 (2011))).

140. *Data Analytics Services*, DO NOT PAY, https://donotpay.treas.gov/dataanalytics.htm (last updated Dec. 15, 2016, 1:14 PM) (describing how the service uses personal information to locate instances of fraud).

141. Ranjit Bose, *Advanced Analytics: Opportunities and Challenges*, 109 INDUS. MGMT. & DATA SYS. 155, 167 (2009) (discussing that commercial profiling is often used to demonstrate the value of data mining). "[P]rofiling consists of identifying homogeneous groups" that "exhibit similar patterns of behavior." *Id.* Profiles (or segments) can be used to develop "predictive or statistical models" to forecast certain behaviors. *Id.* at 168. Government profiling would operate in a similar manner and, in fact, the government flirted with such a profiling platform in 2004 with the Computer Assisted Passenger Prescreening System II. *See* SOLOVE, *supra* note 10, at 182

knowledge-based marketing, profiling presents one of three "major areas of application of data mining,"[142] with the other two being trend and deviation analysis.[143] The Do Not Pay Analytics Services already advertises that it "analyzes data and trends" and engages in "conduct reporting,"[144] both of which parallel the aims of trend and deviation analysis.[145] Developing profiles and "discovering"[146] new information about fraudsters surely presents an attractive, albeit dubious,[147] data mining application to further Do Not Pay's fight against improper payments.[148]

(discussing CAPPS II's airline passenger profiling). CAPPS II was quickly scrapped though due to its failure to address eight key issues, including concerns for privacy. *See* U.S. GEN. ACCOUNTING OFF., GAO-04-385, AVIATION SECURITY: COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES 13 (2004) (providing a table of eight key issues); Jeff Milchen & Jeffrey Kaplan, *The Dangerous Illusion of CAPPS II*, RECLAIM DEMOCRACY!, http://reclaimdemocracy.org/civil_rights_capps_2_illusion_safety (last updated July 2004) (announcing the scrapping of CAPPS II).

142. Michael J. Shaw et al., *Knowledge Management and Data Mining for Marketing*, 31 DECISION SUPPORT SYS. 127, 133 (2001).

143. *Id.*

144. *What Can the Do Not Pay Business Center Do for Your Agency?*, *supra* note 5.

145. *See* Shaw, *supra* note 142, at 134 ("A deviation can be an anomaly (fraud) or a change [in behavior]. . . . Trends are patterns that persist over a period of time. Trends could be short-term . . . . Or, trends could be long-term . . . ."). Data mining employs a suite of tools for identifying deviations and trends over time. *Id.*

146. *See* King & Forder, *supra* note 139, at 699–700 ("In Big Data, data analytics may be used to produce new data that goes beyond simply collecting and aggregating individual pieces of consumer data that are already contained in an existing database . . . . When multiple sources of data are combined into very large datasets for analysis, it is possible to make inferences or draw conclusions about individuals that would not otherwise be retrievable from the datasets. . . . This article uses the term 'discovered data' to refer to the types of new information that may be produced by applying data analytics to datasets available in Big Data . . . .").

147. *See* SOLOVE, *supra* note 10, at 181 ("Of course, profiles can be mistaken, but they are often accurate enough to tempt people to rely on them."). While profiling presents a host of technological and data-related concerns, see *infra* notes 150–55, profiling is also of dubious nature because of the obvious privacy concerns. *See* King & Forder, *supra* note 139, at 696 ("Governments and commentators around the world are wondering how to best protect consumers' privacy in the world of Big Data."). While King and Forder discuss profiling from a consumer perspective, the concerns to individual privacy are no less real when it is the government engaging in big data discovery and analytics programs, rather than a private sector actor. Perhaps it is for that very reason that these concerns are even more pressing and worthy of robust discussion. *See supra* note 141 (discussing CAPPS II).

148. *See* Bose, *supra* note 141, at 167 (discussing, among other benefits, how profiling increases companies' marketing effectiveness by teaching companies how to target certain customers). While this is a private sector application, such a benefit would seem of obvious value to Do Not Pay decision-makers in the fight against fraud and improper payments. *See What Can the Do Not Pay Business Center Do for Your Agency?*, *supra* note 5 (describing Do Not Pay's "commit[ment] to providing . . . cutting edge data analytics"). The possibility that profiling is an attractive option is bolstered by the fact that the government has historically used various data mining techniques to root out fraud. *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 317 (2008).

The problem with profiles is that they can be wrong, inaccurate, or mistaken.[149] Profiling supports decision-making based on past data, which can be stale or incomplete.[150] While speculative, it is possible that Do Not Pay's Analytics Services could inaccurately profile an individual as a fraudster.[151] That profile, in turn, could lead to an adverse information investigation, a process by which the payment-issuing agency verifies the adverse information that Do Not Pay discovers about the payee.[152] This investigation would require the individual to contest the adverse information, creating unnecessary headache and hassle.[153] Another issue with profiling is that more data does not always lead to better insights.[154] Even as agencies more extensively use Do Not Pay after IPERIA, Do Not Pay's profiling capabilities may not experience a corresponding improvement. Rather, Do Not Pay's profiling capabilities may plateau, and the plateau may not be particularly effective or accurate.

Finally, changing purposes and uses of the Do Not Pay program present a cognizable Kafkaesque danger.[155] As Solove points out, data obtained by the government for one purpose may readily be used for a different purpose as motives change.[156] For Do Not Pay, as IPERIA facilitates agency use of Do Not Pay's automated investigation capabilities, the possibility increases that another governmental agency will find other purposes for the Do Not Pay

149. SOLOVE, *supra* note 10, at 181.

150. *See id.*; *see also* Jordan Ellenberg, *What's Even Creepier Than Target Guessing That You're Pregnant?*, SLATE (June 9, 2014, 12:10 PM), http://www.slate.com/blogs/how_not_to_be_wrong/2014/06/09/big_data_what_s_even_creepier_than_target_guessing_that_you_re_pregnant.html ("It's no big deal if Netflix suggests the wrong movie to you. But in other domains, bad data is more dangerous. Think about algorithms that try to identify people with an elevated chance of being involved in terrorism, or people who are more likely than most to owe the government money.").

151. SOLOVE, *supra* note 10, at 181 ("[T]he use of profiling to form predictive models of human behavior incorrectly assumes that the identity of the individual can be reduced, captured, or represented by measurable characteristics. . . . [A] profiled individual is necessarily labeled and henceforth seen as a member of a group, the peculiar features of which are assumed to constitute her personal characteristics."). Someone who is inadvertently profiled as a fraudster may unnecessarily face "considerable hassle and delay." *Id.* at 182.

152. "Before adverse action is taken against an individual, any adverse information that agencies discover shall be subjected to investigation and verification . . . ." OMB MEMORANDUM M-13-20, *supra* note 21, at 11. "Verification requires a confirmation of the specific information that would be used as the basis for an adverse action against an individual." *Id.*

153. "Once agencies have verified the adverse information, they shall provide the individual with notice and an opportunity to contest before taking adverse action." *Id.* "Individuals shall have 30 days to respond to a notice of adverse action, unless a statute or regulation provides a different period of time." *Id.* at 11–12.

154. *See* Laura Patterson, *More Data Does Not Equal Better Insights*, MARKETINGPROFS (June 19, 2013), http://www.marketingprofs.com/articles/2013/11005/more-data-does-not-equal-better-insights.

155. SOLOVE, *supra* note 10, at 184.

156. *Id.*

program, such as financial crime investigation.[157] This possibility is bolstered by Do Not Pay's ability to combine government and commercial data sources, creating new and unique datasets to investigate.[158] Changing purposes and uses of Do Not Pay could engender more government data aggregation and computer matching, further implicating individual privacy interests.

2. IPERIA Mitigates Kafkaesque Dangers, but Concerns Remain

Recognizing that IPERIA likely raises Kafkaesque dangers, this Note argues that a risk analysis is necessary to understand the threat of these dangers to individual privacy interests.[159] If there is a high risk that these dangers will occur, IPERIA poses a threat to individual privacy interests. A low risk, by contrast, means IPERIA does not significantly threaten individual privacy. To determine the risk level, this Note weighs IPERIA's Kafkaesque dangers against its mitigating factors.[160] Mitigating factors would tend to reduce the risk level posed from IPERIA's Kafkaesque dangers, thereby reducing the threat to individual privacy.[161] IPERIA has two primary mitigating factors: its scope and privacy safeguards.[162]

First, IPERIA's purpose illustrates its narrow scope—IPERIA's specific purpose is to address improper payments and the complex issues

---

157. For example, the U.S. Treasury maintains the Financial Crimes Enforcement Network ("FinCEN"), designed to "safeguard the financial system from illicit use and combat money laundering." *See Mission*, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/about/mission (last visited Mar. 15, 2017). Given the breadth of data within Do Not Pay, FinCEN would almost certainly benefit from a partnership.

158. "Section 5(d)(2)(C) of IPERIA provides that the DNP Initiative may include the use of or access to commercial databases to investigate activities for fraud and systematic improper payments detection. Some commercial databases may help the Federal Government meet the objectives of the DNP Initiative." OMB MEMORANDUM M-13-20, *supra* note 21, at 12. Other commentators have expressed concern about this capability, calling for additional OMB guidance on how the government treats privacy protections around commercial database designations. *See generally* ROBERT GELLMAN & PAM DIXON, WORLD PRIVACY FORUM, DATA BROKERS AND THE FEDERAL GOVERNMENT: A NEW FRONT IN THE BATTLE FOR PRIVACY OPENS (2013), http://www.worldprivacyforum.org/wp-content/uploads/
2013/10/WPF_DataBrokersPart3_fs.pdf.

159. An extensive discussion of risk analysis methodology is beyond the scope of this Note. However, the type of risk analysis proposed is based on PMBOK's Qualitative Risk Analysis Technique: Risk Probability and Impact Assessment. *See* PROJECT MGMT. INST., *supra* note 115, at 330. A risk probability assessment investigates the likelihood a risk will occur while a risk impact assessment investigates the potential effects of such a risk. Generally, once a risk probability and impact assessment is completed, the risk is categorized according to a probability and impact matrix. *Id.* at 331.

160. "Risk mitigation is a risk response strategy" that "reduce[s] the probability of occurrence or impact of a risk." *Id.* at 345. Risk mitigation implies a reduction in the impact of an adverse risk. *Id.*

161. *See id.*

162. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390 (2013).

surrounding improper payments.[163] The scope of this purpose further narrows when looking at IPERIA's Privacy Act changes related to the multilateral CMA and Do Not Pay.[164] Since IPERIA allows the multilateral CMA process for Do Not Pay matching programs only, IPERIA retains the Privacy Act's default posture on CMAs for all other agencies.[165] IPERIA could have exempted Do Not Pay from CMA requirements altogether, thereby eliminating all Privacy Act protection.[166] Instead, it arguably creates a program-level approach to the CMA process.[167]

Second, IPERIA contains individual safeguards to protect privacy interests. For example, section 5 requires program transparency through annual reporting requirements on Do Not Pay's operations, including an evaluation of whether Do Not Pay reduces improper payments.[168] Section 5 also requires OMB to establish guidance on data quality issues involving the retention, timely destruction, and correction of Do Not Pay's data in accordance with the Privacy Act.[169] This guidance is a critical safeguard, as maintaining high data quality is important in any computer program, but particularly where automated investigations are occurring.[170] Finally, Section 5 gives OMB authority to develop new guidance for the data integrity boards to: (1) "improve the effectiveness and responsiveness"; (2) "ensure privacy protections in accordance with the Privacy Act"; and (3) "establish standard matching agreements for use when appropriate."[171]

As previously discussed, the data integrity boards are the approving bodies for new matching programs.[172] Among other responsibilities, the Privacy Act charges the data integrity boards with annual reporting on

163. *Id.*

164. *Id.* § 5(e)(2)(d).

165. *See id.*; OMB MEMORANDUM M-13-20, *supra* note 21, at 14 ("Section 5(e)(2)(D) of IPERIA authorizes CMAs 'governing multiple agencies' for purposes of the DNP Initiative. Agencies' default for a matching program shall always be traditional CMAs between one source agency and one recipient agency." (footnote omitted)).

166. 28 C.F.R. § 16.70–16.136 (2016) (listing 66 systems of records that are exempted from certain Privacy Act requirements); *see also* Privacy Act of 1974, 5 U.S.C. § 552a(j)–(k) (2012) (detailing system of record exemption requirements).

167. A program is defined as "[a] group of related projects, subprograms, and program activities managed in a coordinated way to obtain benefits not available from managing them individually." PROJECT MGMT. INST., *supra* note 115, at 553. The idea that a multilateral CMA raises the CMA process from the "project" level to the "program" level helps in conceptualizing how a CMA works across multiple agencies. Each agency's CMA is, in essence, a project and the multilateral CMA brings them together in a program-level approach. *Id.* *See generally* OMB MEMORANDUM M-13-20, *supra* note 21.

168. Improper Payments Elimination and Recovery Improvement Act of 2012 § 5.

169. *Id.* § 5(e)(3).

170. THOMAS N. HERZOG ET AL., DATA QUALITY AND RECORD LINKAGE TECHNIQUES 7–10 (2007).

171. Improper Payments Elimination and Recovery Improvement Act of 2012 § 5(e).

172. *See supra* note 69 and accompanying text (discussing the role and responsibilities of data integrity boards).

certain key topics, such as: (1) proposed matching agreements that the board disapproved; (2) changes in board membership or structure; and (3) alleged or identified violations of matching agreements and any corrective action taken.[173] Data integrity boards must also provide guidance to their agency constituents on matching program requirements.[174]

Following IPERIA, OMB's M-13-20 guidance further clarifies that each payment-issuing agency's data integrity board must review any CMA that an agency enters into with Do Not Pay.[175] Moreover, whenever agencies enter into a multilateral CMA, the data integrity boards are responsible for ensuring that, if a single agency is designated to perform the CMA reporting requirements, the designation of that agency is appropriate.[176] This means that instead of all agencies performing the required CMA reporting, one agency may be designated to report for all agencies involved in the multilateral CMA.[177] Finally, M-13-20 tasks the data integrity boards with ensuring CMAs fully comply with the Privacy Act before they approve any new proposed matching program.[178]

IPERIA's message about the data integrity boards is clear: these boards are the frontline for enforcing Privacy Act protections, particularly with respect to Do Not Pay.[179] Successful board performance is therefore critical to ensuring a proper balance between administrative efficiency and individual privacy interests.[180] With this goal in mind, the M-13-20 guidance outlines new data integrity board requirements to ensure each board performs its duties effectively and responsively.[181] This guidance includes new requirements for annual meetings, board member training on the Privacy Act, and oversight responsibilities for the Senior Agency Official for Privacy ("privacy officer"),[182] who is responsible for an agency's "compliance

173. Privacy Act of 1974, 5 U.S.C. § 552a(u)(3)(D) (2012).

174. *Id.* § 552a(u)(3)(F).

175. OMB MEMORANDUM M-13-20, *supra* note 21, at 10 ("The specific terms of the DNP matching program shall be described in the CMA and reviewed by each payment-issuing agency's [data integrity board].").

176. *Id.* at 14.

177. *Id.* ("Whenever agencies enter into a multilateral CMA, each of the payment-issuing agencies is responsible for meeting the reporting and publication requirements associated with the matching program. However, the payment-issuing agencies may designate a single agency to report the CMA to OMB and Congress and publish the notice in the Federal Register on behalf of the other agencies, if such designation is clear in the report and notice. Each agency's [data integrity board] shall review the designation and determine that the arrangement is sufficient to meet the requirements in the Privacy Act and provide adequate notice to the public." (footnote omitted)).

178. *Id.* at 15.

179. *See* Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, § 5(e)(3)(B), 126 Stat. 2390, 2395 (2013).

180. *See id.*

181. OMB MEMORANDUM M-13-20, *supra* note 21, at 15–16.

182. *Id.*

with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act."[183]

IPERIA significantly mitigates the risk level of Do Not Pay's Kafkaesque dangers.[184] IPERIA's narrow scope and individual privacy safeguards clearly demonstrate Congress' concern for individual privacy interests.[185] To that end, IPERIA lays a solid foundation for privacy protection measures even as it opens the door to new administrative efficiencies.[186] However, OMB's M-13-20 guidance is neither clear enough nor goes far enough in building upon that foundation. This shortcoming is particularly true when it comes to the data integrity boards and the qualifying test for a multilateral CMA. This Note now calls on OMB to take additional measures to ensure against the risk of Kafkaesque dangers as Do Not Pay engages in more automated investigation activities post-IPERIA.

IV. OMB SHOULD ISSUE ADDITIONAL GUIDANCE

As previously discussed, the multilateral CMA is a groundbreaking development and raises concerns that the government is eschewing Privacy Act requirements for administrative efficiency. OMB's M-13-20 guidance was an important first step in alleviating this concern, but more guidance is necessary to ensure that agencies do not abuse the multilateral CMA. The lack of specificity in the M-13-20 guidance creates ambiguities in how the data integrity boards effectively approach their role and how agencies engage in the multilateral CMA process.

To ensure these ambiguities do not elevate to Kafkaesque dangers, OMB should achieve the following three objectives with the data integrity boards through new guidance: (1) increase board effectiveness by implementing new, or updating current, operational requirements; (2) establish annual recertification requirements for Privacy Act training; and (3) require effectiveness assessments in conjunction with the privacy officer. Finally, OMB should define what "sufficiently similar" means in the multilateral CMA qualifying test.[187]

---

183. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-05-08, DESIGNATION OF SENIOR AGENCY OFFICIALS FOR PRIVACY 1 (2005). This individual is defined as "the senior official who has the overall agency-wide responsibility for information privacy issues." *Id.* He or she is charged with a "a central role in overseeing, coordinating, and facilitating the agency's compliance efforts" and "must also have a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information." *Id.* at 2; *see also infra* Part IV.C.

184. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012.

185. *See generally id.*

186. *See generally id.*

187. *See supra* notes 96–97 and accompanying text.

A. INCREASE DATA INTEGRITY BOARD EFFECTIVENESS ON THREE FRONTS

Data integrity boards decide whether to establish a proposed matching program—a critical role in privacy protection.[188] This role is particularly important after IPERIA, which calls for new OMB guidance on board effectiveness in ensuring matching programs comply with the Privacy Act.[189] Effectiveness is defined as "the degree to which something is successful in producing a desired result,"[190] and a desired result of IPERIA is for the boards to protect individual privacy while overseeing new administrative efficiency in the multilateral CMA process.[191] To achieve both ends effectively, the boards must do more than what the M-13-20 guidance contemplates.[192] The following three requirements will increase board effectiveness:
(1) semiannual board meetings; (2) interagency knowledge sharing; and (3) regular strategic planning.

1. Semiannual Board Meetings

OMB should require the data integrity boards to meet internally at least semiannually rather than the annual meeting required in the M-13-20 guidance.[193] Given the importance of the board, and the gravity of issues the board faces when deciding on new matching programs, meeting once a year is simply not enough.[194] While OMB does provide that the boards should "meet with sufficient frequency to ensure that matching programs are carried out efficiently, expeditiously, and in compliance with the law," this guidance is largely a subjective standard that data integrity boards might neglect or flat-out ignore.[195] Requiring semiannual or even quarterly meetings in some cases will ensure the data integrity board takes its role as

188. OMB MEMORANDUM M-13-20, *supra* note 21, at 15.

189. Improper Payments Elimination and Recovery Improvement Act of 2012 § 5(e)(3).

190. *Effectiveness*, NEW OXFORD AMERICAN DICTIONARY (3d ed. 2010).

191. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012.

192. *See* OMB MEMORANDUM M-13-20, *supra* note 21, at 15–16.

193. *Id.* at 15.

194. It is actually a somewhat ironic criticism that this board is not required to meet *enough*, given the propensity of government bureaucracy to create unnecessary meetings as a measurable output of time and energy. ARYE L. HILLMAN, PUBLIC FINANCE AND PUBLIC POLICY: RESPONSIBILITIES AND LIMITATIONS OF GOVERNMENT 218 (2003). Nonetheless, drawing from the corporate world, plenty of literature indicates effective boards should (and do) meet more than once a year. *See, e.g.*, COLIN B. CARTER & JAY W. LORSCH, BACK TO THE DRAWING BOARD: DESIGNING CORPORATE BOARDS FOR A COMPLEX WORLD 144 (2004) (U.S. boards meet on average seven times a year); MARK DALY, 5 STEPS TO BOARD SUCCESS!: NEW APPROACHES TO BOARD EFFECTIVENESS AND BUSINESS SUCCESS 158 (2005) (calling for at least four but up to 12 meetings a year); THEORY AND PRACTICE OF CORPORATE SOCIAL RESPONSIBILITY 46 (Samuel O. Idowu & Céline Louche eds., 2011) (boards meeting at least quarterly and sometimes monthly).

195. OMB MEMORANDUM M-13-20, *supra* note 21, at 15.

seriously as IPERIA contemplates.[196] More importantly, it will facilitate responsiveness in board determinations on proposed matching programs—a general effectiveness goal of M-13-20.[197]

2. Interagency Knowledge Sharing

OMB should require the data integrity boards to engage in interagency knowledge sharing activities. Knowledge sharing is the process of converting knowledge "into a form that can be understood, absorbed, and used by other individuals."[198] Knowledge sharing moves knowledge to the organizational level where it is transformed into organizational value and collectively shared.[199] Most importantly, knowledge sharing "provides strategic advantages for government to improve decision-making and enhance the quality of services and programs."[200]

Requiring interagency knowledge-sharing activities amongst the data integrity boards would benefit individual privacy protection and administrative efficiency. For example, knowledge sharing allows dissemination of board best practices[201] and lessons learned.[202] Knowledge sharing also facilitates informal relationship building, something that may prove valuable for the boards as agencies collaboratively engage in the multilateral CMA process.[203] Finally, knowledge sharing may help the boards identify issues with proposed matching programs more quickly and more

196. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012. A semiannual meeting will ensure that the boards still have time to sufficiently plan for the meeting, while also not falling victim to over-meeting unnecessarily. *See supra* note 194 and accompanying text (discussing government propensity to schedule too many meetings). A quarterly meeting may be more appropriate for those agencies with frequently sought-after data sources, such as the Death Master File or the Excluded Parties List. *See supra* notes 40–41 and accompanying text.

197. OMB MEMORANDUM M-13-20, *supra* note 21, at 15–16.

198. Minu Ipe, *Knowledge Sharing in Organizations: A Conceptual Framework*, 2 HUM. RESOURCE DEV. REV. 337, 341 (2003).

199. *Id.* at 342.

200. Jing Zhang et al., *Exploring Stakeholders' Expectations of the Benefits and Barriers of E-Government Knowledge Sharing*, 18 J. ENTERPRISE INFO. MGMT. 548, 549 (2005).

201. "[T]he policy, systems, processes, and procedures that, at any given point in time, are generally regarded by peers as the practice that delivers the optimal outcome, such that they are worthy of adoption." WILLIS H. THOMAS, THE BASICS OF PROJECT EVALUATION AND LESSONS LEARNED 62 (2d ed. 2015) (quoting N.Z. CONSTR. INDUS. COUNCIL, PRINCIPLES OF BEST PRACTICE: CONSTRUCTION PROCUREMENT IN NEW ZEALAND 2 (2006)).

202. "Lessons learned are defined as key project experiences which have a certain general business relevance for future projects. They have been validated by a project team and represent a consensus on a key insight that should be considered in future projects." Martin Schindler & Martin J. Eppler, *Harvesting Project Knowledge: A Review of Project Learning Methods and Success Factors*, 21 INT'L J. PROJECT MGMT. 219, 220 (2003).

203. *See* Richard McDermott & Carla O'Dell, *Overcoming Cultural Barriers to Sharing Knowledge*, 5 J. KNOWLEDGE MGMT. 76, 82 (2001) (discussing that many "informal human networks" form around knowledge sharing activities).

effectively than they might otherwise have by operating in a vacuum.[204] How the boards actually engage in knowledge-sharing activities should be left for each to decide;[205] however, OMB should broadly require (and facilitate where needed) such activities, as well as routine reporting on knowledge sharing successes and challenges.

3. Strategic Planning

The goal of strategic planning is to increase board effectiveness generally, thereby increasing assurance that the boards will respect individual privacy protections as they carry out their role. Thus, OMB should require the data integrity boards to engage in regular strategic planning to encourage effective decision-making and operations.[206] While some boards may already engage in strategic planning activities, establishing it as a requirement sends the signal that OMB expects all boards to be effective bodies within their respective agencies.[207] To support this requirement, OMB should establish a broad topic framework for the boards to utilize. This framework should include, at a minimum, general board operating procedures such as succession planning, matching program review processes, and strategies to effectively meet the various board reporting obligations.

---

204. *See* Joe Correia, *Data Governance: 5 Common Pitfalls and How to Avoid Them*, DAYMARK (Oct. 2, 2015), http://www.daymarksi.com/information-technology-navigator-blog/data-governance-5-pitfalls-and-how-to-avoid-them (discussing the data governance pitfall of "siloed team[s]," "operat[ing] in a vacuum," and implementing projects that impact the entire enterprise). In the case of the data integrity boards, the stakeholder base is necessarily broader than just the agency as an enterprise, given the personal information involved in the proposed matching program. As such, the need for informed decision-making is absolutely critical. *See infra* note 217 and accompanying text (defining "stakeholder").

205. In practice, knowledge sharing could be as simple as OMB disseminating minutes, missives, or memoranda from well-functioning data integrity boards as a way to provide insight into successful board architecture and practices. More complex knowledge sharing may involve OMB playing a central coordinating role for regular data integrity board summits, or developing playbooks or "rules of the road" for all data integrity boards based on a composite of success stories and lessons learned from data integrity board deliberation and decision-making. Knowledge sharing could even involve a secure portal for the data integrity boards, allowing document management, interactive discussion, and question and answer forums. The overall goal is to break down silos and get boards talking. *See supra* note 204 and accompanying text (discussing data silos).

206. "Strategic planning is an organizational management activity that is used to set priorities, focus energy and resources, strengthen operations, ensure that employees and other stakeholders are working toward common goals, establish agreement around intended outcomes/results, and assess and adjust the organization's direction in response to a changing environment." *Strategic Planning Basics*, BALANCED SCORECARD INST., http://balancedscorecard.org/Resources/Strategic-Planning-Basics (last visited Mar. 15, 2017).

207. *Id.*

B. *ESTABLISH ANNUAL RECERTIFICATION REQUIREMENTS FOR THE DATA INTEGRITY BOARDS*

OMB's M-13-20 guidance directs each agency's privacy officer to develop a training program for board members on Privacy Act-related issues.[208] The training must include information on "the requirements in the Privacy Act, other relevant laws, and guidance from OMB, [National Archives and Records Administration], and the Department of Commerce's National Institute of Standards and Technology."[209] While some agencies' privacy officers may be able to establish a successful training program, OMB should take a more proactive role in ensuring all of the data integrity boards are properly trained in these areas. Allowing each agency's privacy officer to develop the program for each agency raises concerns of training variation, subjectivity, and incompleteness.

OMB should therefore develop its own training program through an annual certification.[210] By standardizing[211] the data integrity board training in this way, OMB will best uphold IPERIA's intent for the boards to ensure privacy protections are met by helping the boards be as adequately informed as possible on the Privacy Act and other relevant laws.[212] The benefit of a certification program is that it ensures board members have met OMB's specific requirements to perform their role.[213] Moreover, requiring annual recertification is an effective way for the boards to remain trained on the government and industry standards critical to their role, such as data

---

208. OMB MEMORANDUM M-13-20, *supra* note 21, at 15.

209. *Id.*

210. Regarding certification:

> Certification is a process by which key required competencies for practice are measured, and the professional endorsed by a board of his/her peers. This process serves to enhance the credibility of the qualifying professional, thus assuring the consumer, be it an individual or an organization, that the individual has been approved by a recognized authority.

Rosemary M. Lysaght & James W. Altschuld, *Beyond Initial Certification: The Assessment and Maintenance of Competency in Professions*, 23 EVALUATION & PROGRAM PLAN. 95, 96 (2000) (citation omitted).

211. *Id.* ("The board holds responsibility for determining standards and requirements as appropriate . . . for initial and continuing eligibility . . . ."). Thus, as a practical matter, OMB should establish some form of a working group or committee that acts as a certification board for the data integrity boards, developing and promulgating standard requirements for data integrity board initial certification and recertification.

212. *See* Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, § 5(e)(3)(B), 126 Stat. 2390, 2395 (2013) (calling for OMB to review the procedures of the data integrity boards and develop new guidance to ensure privacy protections are met in accordance with the Privacy Act).

213. To be certified in something means "having met the official requirements that are needed to do a particular type of work" or "officially approved as having met a standard." *Certified*, MERRIAM-WEBSTER: LEARNER'S DICTIONARY, http://www.learnersdictionary.com/definition/certified (last visited Mar. 15, 2017).

handling, retention, destruction, and correction.[214] As these standards evolve over time, an annual recertification requirement will ensure that board members remain abreast of key changes.[215]

A potential downside of this approach is that it may create internal conflict between OMB and the agencies' privacy officers over their efforts to develop training materials after OMB initially issued its M-13-20 guidance. To alleviate these concerns, OMB should involve interested privacy officers as subject matter experts[216] and stakeholders[217] wherever possible. A collaborative approach between OMB and the privacy officer will ensure that the process captures lessons learned and best practices,[218] while reducing the chances of internal conflicts. Once OMB develops the certification training, OMB should once again leverage these privacy officers to ensure data integrity board members complete annual recertification requirements in a timely manner.

C. REQUIRE DATA INTEGRITY BOARDS TO SELF-ASSESS THEIR EFFECTIVENESS WITH THE PRIVACY OFFICER

OMB's M-13-20 guidance grants the privacy officer an important oversight role. M-13-20 requires the privacy officer to "periodically review the effectiveness and responsiveness" of the data integrity board and then determine whether the board needs additional guidance.[219] But OMB provides no information on how the privacy officer should determine whether additional guidance is needed.[220] OMB also does not address potential conflicts of interest that exist between the data integrity boards

214. "A continuous review process should be established to examine the competency standards upon which evaluation procedures are based. This process must be sensitive to changes in the field and its technologies, and draw on research related to best practice." Lysaght & Altschuld, *supra* note 210, at 103; *see also* Improper Payments Elimination and Recovery Improvement Act of 2012 § 5(e)(3)(B).

215. Lysaght & Altschuld, *supra* note 210, at 103.

216. "A subject matter expert, or SME, is a 'person with bona fide expert knowledge about what it takes to do a particular job.'" Frequently Asked Questions: Assessment Policy, OPM, https://www.opm.gov/FAQs (last visited Mar. 15, 2017) (quoting U.S. Office of Pers. Mgmt., Delegated Examining Operations Handbook: A Guide for Federal Agency Examining Offices (2007), https://www.opm.
gov/policy-data-oversight/hiring-information/competitive-hiring/deo_handbook.pdf).

217. *See* PROJECT MGMT. INST., *supra* note 115, at 563 (defining a stakeholder as "[a]n individual, group, or organization who may affect, be affected by, or perceive itself to be affected by a decision, activity, or outcome of a project").

218. The privacy officers should have agency-specific insights and experience when it comes to developing training materials. As the privacy officers are closest to IPERIA's target audience for ongoing privacy training efforts (i.e. the data integrity boards of each agency), their experiences developing training materials should prove valuable to OMB as it centralizes a certified training process. OMB should therefore leverage the privacy officers' experiences in developing training protocols to improve their training materials and dissemination efforts.

219. OMB MEMORANDUM M-13-20, *supra* note 21, at 15–16.

220. *See id.*

and the privacy officer, even though the two roles are within the same agency.[221] To alleviate these concerns, OMB should issue new guidance that requires the data integrity boards to self-assess their effectiveness collaboratively with the privacy officer, using an objective framework or checklist.

Assessing effectiveness can be a complex and rigorous process.[222] However, a growing body of research has developed regarding governance best practices and organizational effectiveness.[223] OMB should take advantage of this research and promulgate an assessment tool based on leading research in this field, or adapt for use an existing self-assessment tool, such as the Governance Self-Assessment Checklist, Board Self-Assessment Questionnaire, or the Benchmarks of Excellence tool.[224] In either case, requiring the data integrity boards to assess their effectiveness in partnership with the privacy officer should result in several benefits.

First, a collaborative assessment of effectiveness directly involves the privacy officer in the process of identifying and rating various board strengths, weaknesses, and internal challenges.[225] This involvement should naturally result in better insights and greater information sharing amongst the boards and privacy officers regarding board effectiveness. Better insights and greater information sharing will allow the privacy officer to report more knowledgably to OMB about data integrity board effectiveness and responsiveness, pursuant to OMB's M-13-20 guidance.[226] Second, bringing the privacy officer into the board self-assessment process brings in a perspective outside of the board, which can result in a more insightful

221. A conflict of interest is "[a] situation that has the potential to undermine the impartiality of a person because of the possibility of a clash between the person's self-interest and professional interest or public interest." *Conflict of Interest*, BUSINESSDICTIONARY, http://www.businessdictionary.com/definition/conflict-of-interest.html (last visited Mar. 15, 2017). This includes, but is not limited to, fear of retaliation, willful blindness, or some other obstruction of privacy officer duties. *See generally* Susan M. Heathfield, *Conflict of Interest: See Examples of Potential Workplace Conflicts of Interest*, BALANCE, https://www.thebalance.com/conflict-of-interest-1918090 (last updated Jan 28, 2017).

222. *See* Mel Gill et al., *The Governance Self-Assessment Checklist: An Instrument for Assessing Board Effectiveness*, 15 NONPROFIT MGMT. & LEADERSHIP 271, 272 (2005) ("Notwithstanding the complexities of rigorous organizational effectiveness evaluation, a small but growing body of research has identified governance best practices and examined the relationship of the latter with effective organizational performance.").

223. *Id.*

224. *Id.* at 274.

225. A simple, yet effective example of this process is "The Governance Effectiveness Quick Check." *See id.* at 292. The data integrity board could complete this quick check and then collaboratively discuss the results with the privacy officer.

226. OMB MEMORANDUM M-13-20, *supra* note 21, at 16.

assessment.[227] These benefits should translate into a qualitative improvement in privacy officer oversight.

As the quality of the privacy officer's oversight improves, so too should the level of confidence that the boards are carrying out their role effectively. As data integrity boards are the frontline for ensuring that the government respects and enforces the Privacy Act, proper privacy officer oversight is critical to ensuring the boards are effective in managing new administrative efficiencies through the multilateral CMA. OMB should empower each agency's privacy officer, to the greatest extent possible, to carry out his or her oversight mission. Requiring a closer partnership between the data integrity boards and the privacy officers through a collaborative self-assessment of board effectiveness is a powerful measure to ensure that the privacy officer has effective oversight.

D. DEFINE WHAT "SUFFICIENTLY SIMILAR" MEANS IN THE CONTEXT OF DATA ELEMENTS

As previously discussed, the multilateral CMA allows for more efficient access to restricted personal information content in Do Not Pay, resulting in increased automated investigation of agency payees through computer matching.[228] The multilateral CMA, therefore, enhances administrative efficiency, but it does not add anything by way of individual privacy protection.[229] Recognizing this deficiency, OMB's M-13-20 guidance erects a countervailing privacy protection hurdle for the multilateral CMA in the form of a qualifying test requiring "the matching purpose and the specific data elements" to be "sufficiently similar."[230] However, the test misses the mark in a critical way: OMB does not define what it means by "sufficiently similar."[231]

A data integrity board could interpret this "sufficiently similar" requirement broadly or narrowly.[232] A broad reading could imply that individual data elements contained within one dataset must be similar, but not exact, to individual data elements in another dataset to be sufficiently similar. For example, one data set containing a data element titled

---

227. In a corporate context, an emerging best practice for boards assessing their effectiveness is to take into account perspectives beyond just those of the directors. *See* ALICE AU ET AL., IMPROVING BOARD EFFECTIVENESS 3–4 (2012), https://www.spencerstuart.com/~/media/pdf%20files/research%20and%20insight%20pdfs/pov12_indart_boardsnew.pdf. This approach should translate well to privacy officer involvement in data integrity board effectiveness assessment.

228. *See supra* Part III.A.

229. *See* OMB MEMORANDUM M-13-20, *supra* note 21, at 14.

230. *Id.*

231. *See id.* "[A] data element [is] [t]he fundamental data structure in a data processing system. Any unit of data defined for processing is a data element; for example, ACCOUNT NUMBER, NAME, ADDRESS and CITY." *Data Element*, FREE DICTIONARY, http://encyclopedia2.thefreedictionary.com/data+element (last visited Mar. 15, 2017).

232. *See* OMB MEMORANDUM M-13-20, *supra* note 21, at 14.

LAST_FIRST_NAME and another dataset containing the data element LAST_NAME could be sufficiently similar under this reading, as one dataset contains a subset of the other. A narrow reading, however, could require a specified percentage of data elements within an agency's dataset to be *identical* to the data elements contained within another agency's dataset, determined on a case-by-case basis by the reviewing data integrity boards. For example, a data integrity board may determine that between Agencies X, Y, and Z, 30% of their individual data elements must be *identical* to be *sufficiently similar*.

The problem with a broad reading is that it allows a greater number of agencies to satisfy the first prong of M-13-20's test for a multilateral CMA, perhaps improperly. This opens the door for misuse and controverts IPERIA's intent to balance administrative efficiency with privacy protections.[233] To ensure that agencies appropriately use the multilateral CMA, OMB should clarify its M-13-20 guidance by adopting the narrow reading. In requiring agencies to prove their datasets are sufficiently similar by showing a percentage of identical data elements, OMB ensures agencies utilizing a multilateral CMA have a legitimate need. The multilateral CMA should not be an easy or expedient option; rather, it should be an exception to the Privacy Act rules for a CMA.

A narrow reading also gives data integrity boards the ability to establish the required percentage of data elements that must be identical to prove out that the datasets are sufficiently similar. Since agencies will have varying amounts of data elements within their datasets, data integrity boards should individually evaluate each proposed multilateral CMA to determine the appropriate percentage. The boards could take into account such factors as: (1) how many agencies are entering the multilateral CMA; (2) the size of each agency's dataset; and (3) the desired level of individual privacy protection.[234] As a general rule, requiring a higher percentage of identical data elements will translate to greater individual privacy protection.[235] OMB

233. *See generally* Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390 (2013).

234. Other factors could certainly be relevant to this inquiry. However, these factors sufficiently balance individual privacy and administrative efficiency, a central theme of this Note. For example, a small number of agencies (factor 1) with small datasets (factor 2) would tend to weigh against a multilateral CMA, as a regular CMA would likely suffice. Conversely, a large number of agencies with small datasets would tend to weigh in favor of a multilateral CMA, as administrative efficiency would be desirable and the risk of privacy over-exposure with small datasets is lower. Of course, each data integrity board can adjust its desired level of individual privacy protection (factor 3) as a way to arrive at the administrative realities of the situation. Thus, these three factors work together in a discretionary framework that pits individual privacy and administrative efficiency against each other in a deliberative and flexible way.

235. Requiring high percentages of identical data elements will make it difficult for agencies to satisfy the qualifying test. Thus, the higher the required percentage, the less likely

should promulgate new guidance to address this concern and update M-13-20's test accordingly.

V. CONCLUSION

IPERIA is a groundbreaking development in the course of the Do Not Pay program. The ability for several agencies to utilize one multilateral CMA to access restricted personal information content in Do Not Pay portends a new era in automated investigation through computer matching. OMB should guard against the dangers to individual privacy that this new era presents, and the best way to do so is to build upon IPERIA's privacy safeguards. The M-13-20 guidance was a start, but OMB should now promulgate new guidance that strengthens and clarifies M-13-20. Doing so will ensure appropriate use of the multilateral CMA and maintain the balance between administrative efficiency and individual privacy interests. The government should fight hard against improper payments, but it must respect individual privacy while doing so.

an agency will be to use a multilateral CMA. This, in turn, protects individual privacy because it will force the agency to follow the standard CMA process, as outlined in the Privacy Act.