REPORT

POGO.org

PROJECT ON GOVERNMENT OVERSIGHT

Improper Payments:

Data Matching Barriers Prevent Inspectors General From Reaching Full Potential

October 12, 2016
By Nicholas Pacifico

Project On Government Oversight
1100 G St. NW Suite 500
Washington, DC 20005
(202) 347-1122 | www.pogo.org

INTRODUCTION

Over the past few months, the Project On Government Oversight has interviewed various members of the Inspector General (IG) community to better determine the primary issues plaguing the IG system. When asked about the largest barriers preventing them from effectively doing their job, every IG we spoke to mentioned the restrictions placed on their ability to obtain and compare digital information within and across agencies. Our research has found that various laws, and some agency practices, prevent IGs and agencies from effectively sharing and comparing otherwise readily available information. And while the laws discussed below all have legitimate purposes, the ways they are being put into practice have severely hampered the ability of IGs and agencies to pool their resources, reduce redundant work, and perform effective government-wide oversight.

The majority of these restrictions were implemented by or as a result of the Computer Matching and Privacy Protection Act of 1988 (CMPPA),[1] which amends the Privacy Act of 1974 (Privacy Act).[2]

LEGISLATIVE HISTORY

Privacy Act of 1974

The Privacy Act was created in an attempt to regulate the collection, maintenance, use, and sharing of taxpayers' personal information (such as Social Security Numbers) by federal agencies.[3]

It focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies.
2. To grant individuals increased rights of access to agency records maintained about them.
3. To grant individuals the right to seek amendment of agency records maintained about them upon demonstrating that the records are not accurate, relevant, timely, or complete.
4. To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collecting, maintaining, and sharing records.[4]

While its objectives are admirable, the Department of Justice has found that this Act has "imprecise language, a limited legislative history, and somewhat outdated regulations" as of 2015.[5] Even with over 40 years of administrative and judicial analysis, "numerous issues remain

[1] Public Law 100-503.
[2] Public Law 93–579.
[3] Department of Justice, *Overview of the Privacy Act of 1974 (2015 Edition)*, Report p. 1, PDF p. 5. https://www.justice.gov/opcl/file/793026/download (Hereinafter, *Overview of the Privacy Act of 1974)*
[4] *Overview of the Privacy Act of 1974*, Report p. 1, PDF p. 5.
[5] *Overview of the Privacy Act of 1974*, Report p. 1, PDF p. 5.

unresolved or unexplored."[6] These problems make the statute difficult to decipher and apply consistently, especially given the rapid pace at which technology has evolved since its inception.[7]

Computer Matching and Privacy Protection Act of 1988

To address the use of computers and other digital means as the standard way for storing and handling data, and the resulting privacy concerns, Congress implemented the CMPPA. This Act "prevents unregulated government access to personal records for purposes unrelated to the legitimate reasons for which the records were collected."[8] It accomplishes this by establishing standardized ways in which government entities can share information with each other and with state and local governments.[9]

The CMPPA states that, in order to share digital information with other allowable entities, agencies and IGs must legally enter into a formal Computer Matching Agreement (CMA) with each entity it wishes to share information with.[10] A CMA is an official document "that establishes the conditions, safeguards, and procedures" under which a federal organization agrees to disclose data and "where there is a computerized comparison of two or more automated System of Records (SORs)."[11] The Privacy Act defines an SOR "as any grouping of information about an individual under the control of a federal agency from which it retrieves information" by using some personal identifier (such as a Social Security number or an individual's name)[12]—in other words, any database, program, or other system that an agency uses to store and retrieve information about taxpayers.

CMAs are also required to conduct any audits, investigations, evaluations, or inspections where the review methodology includes computerized comparisons that constitute a "matching program" as defined under the Privacy Act.[13] A "matching program" is any computerized comparison of two or more automated SORs for the purpose of:

1. Becoming compliant or maintaining compliance with a statutory or regulatory requirement,

---

[6] *Overview of the Privacy Act of 1974*, Report p. 1, PDF p. 5.
[7] Discussing the entirety of the Privacy Act is a task too large and complex for this report, but the important pieces of the law will be referenced where relevant throughout this report. If you are looking for a more in-depth analysis of the Privacy Act, the Department of Justice does an excellent job of dissecting it in *Overview of the Privacy Act of 1974.*
[8] Letter from Peggy Gustafson, Chair of the Council of the Inspectors General on Integrity and Efficiency, to the Honorable Beth Cobert, Deputy Director for Management of the Office of Management and Budget, about CIGIE's legislative priorities for the 114th Congress, February 20, 2015, p. 2. https://www.ignet.gov/sites/default/files/files/committees/legislative/CIGIE%20Legislation%20Priorities%20-%20114th%20Congress%20Letter.pdf (Hereinafter, CIGIE Legislative Priorities)
[9] 5 U.S.C. Sec. 552a(a)(10).
[10] Public Law 100-503, Section 2(2).
[11] Department of the Treasury, *Do Not Pay Agency Implementation Guide*, December 2014, Report p. 69, PDF p. 73. dhttp://donotpay.treas.gov/DNPAgencyImplementationGuidePublic.pdf
[12] 5 U.S.C. Sec. 552a(a)(5); *Overview of the Privacy Act of 1974*, Report p. 30, PDF p. 34.
[13] CIGIE Legislative Priorities, p. 2.

2. Verifying the eligibility of recipients, beneficiaries, participants, or providers to participate in federal benefit programs,
3. Recouping delinquent, improper, or other types of payments from federal benefit programs, or
4. Comparing federal personnel or payroll information with state and local systems.[14]

The "matching program" language has also been found to apply to IG investigations and audits into their own agency that involve SORs, so IGs are required to get CMAs to access applicable data stored and maintained by the agency they oversee in such instances. It is important to note that the term "matching program" explicitly does not include sharing data for:

1. Statistical analysis that does not use personal identifiers,
2. Research projects where the data is not used to make decisions concerning the rights, benefits, or privileges of specific individuals,
3. Agencies whose primary function is the enforcement of criminal laws,
4. Tax information purposes,
5. Routine administrative purposes relating to federal personnel as long as the purpose of the match does not involve taking any adverse actions against federal personnel, or
6. Foreign counter-intelligence or security clearance purposes.[15]

To assist with the implementation of the CMPPA, the Act requires each agency to create and maintain an internal Data Integrity Board (DIB).[16] These boards consist of senior officials designated by the head of the agency, and may include the IG.[17] The DIB is ultimately responsible for interpreting the CMPPA and providing guidance to its agency and its personnel on the requirements for creating matching programs.[18] DIBs must also approve all CMAs in which their agency is involved.

In short, once an agency or inspector general has created a CMA, the CMPPA requires the inspector general to:

1. Get the CMA reviewed and approved by the DIBs of all agencies involved;
2. Provide a cost-benefit analysis that lays out the justification for the program and the results expected, including the specific estimate of any savings; and
3. If the CMA is approved, notice must be published in the Federal Register at least 30 days prior to when the matching will take place.[19]

If a DIB does not approve the CMA, the IG can appeal to the Director of the Office of Management and Budget (OMB).[20] The Director may approve the matching agreement if he or

[14] 5 U.S.C. Sec. 552a(a)(8)(A)(i)-(ii).
[15] 5 U.S.C. Sec. 552a(a)(8)(b)(i)-(vi).
[16] Public Law 100-503, Section 4.
[17] 5 U.S.C. Sec. 552a(u)(2).
[18] 5 U.S.C. Sec. 552a(u)(3)(F).
[19] CIGIE Legislative Priorities, pp. 2-3.
[20] 5 U.S.C. Sec. 552a(u)(5)(A).

she determines the matching program will be: (1) consistent with all applicable legal, statutory, and policy requirements, (2) cost-effective, and (3) in the public interest.[21]

Having this safeguard is a way to prevent agency abuse of the DIBs in suppressing investigations or access to agency information that is embarrassing or otherwise detrimental to the agency in questions.

Computer Matching and Privacy Protection Amendments of 1990

A series of amendments to the CMPPA were included in the Omnibus Reconciliation Act of 1990—collectively referred to as the Computer Matching and Privacy Protection Amendments of 1990[22]—to address concerns regarding potential abuses of data received through the Act. These amendments implement safeguards by disallowing agencies from making negative decisions against or denying any payment to individuals based on information received via matching agreements unless the agency:

1. Independently verifies the information, or their DIB determines in accordance with the OMB Director that:
    a. The information used was limited to identification information and the amount of benefits paid by the source agency; and
    b. There is a high degree of confidence that the information is accurate; and
2. Provides notice to the individual containing a statement of its findings, and information on how the individual can contest them; and
3. Has waited either:
    a. The time allowed for the individual to respond after receiving notice as set by the federal beneficiary program in question; or
    b. If there is no specific time allotted by the program, 30 days from the date the individual was notified, via mail or otherwise.[23]

Agencies can take any appropriate actions notwithstanding the above if it determines that public health or safety may be "adversely affected" or "significantly threatened" if they do not act prior to the end of the notice period.[24] The amendments also address specifics as to how an agency can independently verify information.

CURRENT PROBLEMS

As stated before, being unable to data-match with other agencies was the most cited barrier preventing IGs from doing their job effectively. The Council of the Inspectors General on Integrity and Efficiency (CIGIE) has found that, even when a DIB approves a CMA, the process

[21] 5 U.S.C. Sec. 552a(u)(5)(B)(i)-(iii).
[22] Public Law 100-503, Section 7201.
[23] 5 U.S.C. Sec. 552a(p)(1)(A)-(C); Public Law 100-503, Section 7201.
[24] 5 U.S.C. Sec. 552a(p)(3).

for setting up a matching agreement has been known to take more than a year to complete.[25] And that is when everything goes right. It can take much longer if the DIB rejects the CMA and the inspector general appeals that decision. Sources have also told POGO that the fear of violating the CMPPA regularly prevents IGs from gaining access to data from agencies who want to work with them or who are mandated by other laws to share such information, let alone agencies who are looking for any excuse not to provide the IGs with said data.

Which raises the problem of independence. If an IG needs information that can only be obtained through a CMA, the CMPPA requires the IG to go through the DIB approval process, leaving approval of the IG's request to the discretion of the leadership of the very agency the IG oversees. This clearly infringes on the independence of IGs. While IGs may be on the DIBs making this decision, as of now they are not required to be, and even if they were they would most likely not be taking part in deciding whether or not to approve their own CMA proposals. POGO has written in depth about the importance of maintaining IG independence, and this is a severe infringement on that independence.[26]

Even removing IGs from the equation, this law is preventing agencies themselves from sharing data with each other. One egregious example is the Department of the Treasury's Do Not Pay List. The List is supposed to contain up-to-date versions of the Social Security Administration's (SSA) Death Master File.[27] But SSA has historically provided Treasury an out-of-date version of this file because it does not believe it has the authority to provide them with access to the complete file, even though the Improper Payment Elimination and Recovery Improvement Act of 2012 requires them to do so.[28] This is a major problem for the Internal Revenue Service, which needs to verify whether individuals are fraudulently using Social Security Numbers of dead individuals to collect various tax benefits.

POTENTIAL SOLUTIONS

One recent law and a current piece of legislation have attempted to address the barriers preventing agencies and IGs from effectively sharing information with one another. While these legislative efforts have not yet been implemented, a close eye should be kept on them in order to make sure they are as effective as possible.

---

[25] CIGIE Legislative Priorities, p. 3.
[26] Project On Government Oversight, *Inspectors General: Many Lack Essential Tools for Independence*, February 26, 2008. http://www.pogo.org/our-work/reports/2008/go-ig-20080226.html; Project On Government Oversight, "Testimony of POGO's Danielle Brian on 'All' Means 'All': The Justice Department's Failure to Comply With Its Legal Obligation to Ensure Inspector General Access to All Records Needed For Independent Oversight," August 5, 2015. http://www.pogo.org/our-work/testimony/2015/testimony-of-pogos-danielle-brian.html; Project On Government Oversight, "Independence of Inspectors General is Essential" September 9, 2016. http://www.pogo.org/blog/2016/09/independence-of-inspectors-general-essential.html
[27] Opening Statement of Senate Homeland Security and Governmental Affairs Committee Chairman Ron Johnson for the full committee hearing, "Examining Federal Improper Payments and Errors in the Death Master File," March 16, 2015. http://www.hsgac.senate.gov/download/?id=20CEA121-9705-4EDF-9981-A0090EAD9B35
[28] Public Law 112-248, Sections 5(a)-(b).

Digital Accountability and Transparency Act of 2014 (DATA Act)

The DATA Act amends the Federal Funding Accountability and Transparency Act of 2006[29] and seeks "to increase accountability and transparency in Federal spending."[30] The DATA Act will eventually create a "Data Analysis Center," or otherwise expand existing services, in order to "provide data, analytics tools, and data management techniques to support" efforts to eliminate improper payments by federal agencies and improve efficiency and transparency in government spending generally.[31] The Secretary of this program may enter into agreements with agencies and IGs to provide data from this center for the "identification, prevention, and reduction of waste, fraud, and abuse related to federal spending," and for use in criminal and other types of investigations.[32]

While the DATA Act has not yet been fully implemented, it has already been enacted into law, and many IGs hope it will facilitate timely access to the data they need to do their job.

Inspector General Empowerment Act of 2016

The Inspector General Empowerment Act of 2016 (IGEA) is proposed legislation, passed in the House, that, in part, would exempt IGs from the CMPPA matching agreement requirements when they are performing investigations, audits, and other core functions of their job.[33] The IGEA specifically exempts the comparison of SORs by IGs from the definition of "matching programs," thus not requiring them to seek out CMAs in order to gain access to data they need to effectively audit or investigate their own and other agencies.

Not only would this solve the independence issues raised by requiring DIB approval of IG CMAs, it should also reduce the total load of CMAs that DIBs need to analyze, and hopefully reduce the time it takes for agencies to get through the CMA approval process. CIGIE and individual IGs have written letters and reports in support of this specific piece of legislation, as well as in support of similar endeavors to exempt IGs from the CMPPA in the past.[34] While we are cognizant of the valuable purposes the Privacy Act and the CMPPA serve, the government needs to create mechanisms that satisfy those purposes while not bringing internal government oversight to an essential standstill.

[29] Public Law. 109-282; 31 U.S.C. 6101 note.
[30] Public Law 113-101, 128 STAT. 1146.
[31] Public Law 113-101, 128 STAT. 1152.
[32] Public Law 113-101, 128 STAT. 1152.
[33] 114 H.R. 2395; 114 S. 579.
[34] Letter from Michael E. Horowitz and Kathy A. Buller, Chairs of the Council of the Inspectors General on Integrity and Efficiency, to the Honorable Ron Johnson and the Honorable Thomas R. Carper, Chairman and Ranking Member of the Senate Committee on Homeland Security and Government Affairs, about CIGIE's support for the Inspector General Empowerment Act of 2015, October 6, 2015. https://www.ignet.gov/sites/default/files/files/CIGIE%20Letter%20re%20IG%20Empowerment%20Act%20Oct%206%202015.pdf; CIGIE Legislative Priorities, pp 2-3.

CONCLUSION

There is still much to do to remedy the information flow blockage that has resulted from the inconsistent interpretations of the complex Privacy Act and CMPPA. The time delays and inability to access data are inhibiting the effective auditing and oversight of the federal government. The DATA Act and the IGEA are steps in the right direction—especially if the IGEA is enacted into law—but they do not fully address the seemingly endless issues the government has with unintentionally or unreasonably inhibiting data-sharing, or with its continued stymieing of IGs.