Gutting the Privacy Act:

Agency use of Systems of Records Notices (SORNs)

Wordcount: 13,831 with footnotes

"By requiring open rule making with the receipt of comments and an agency statement explaining the exception for certain categories of records, the Congress was trying to avoid creation of a loophole which would permit entire agencies to avoid compliance with the Act."[1]

"The agency's broad interpretation would bring through the back door a provision expressly omitted from the Act as approved by Congress and signed into law."[2]

---

[1] James H. Davidson, *The Privacy Act of 1974—Exceptions and Exemptions*, 34 FED. BAR J. 279 (1975), *available in* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, SOURCE BOOK ON PRIVACY, 1191, 1193 (1976) [hereinafter Davidson *Privacy Act*].

[2] *Vymetalik v. F.B.I.*, 785 F.2d 1090, 1095 (C.A.D.C. 1986).

Introduction

The collection and analysis of personal data drives the Internet economy—the idea being that the more you know about individuals, the more you can predict their behavior, and the more closely you can provide the products they desire.[3] With the growth of data gathering and data mining in the private sector, it is only natural that the United States government would want to harness these tools, touted as effective, for its own purposes. These government purposes range from the administration of Social Security benefits to counter-terrorism activities.[4]

In the realm of intelligence gathering, at least, data mining raises serious concerns: it inevitably produces false positives, which are far more dangerous when they indicate that an individual is a terrorist than when they indicate that he likes chicken soup. The surveillance-like aspects of data mining also have troubling implications for a democratic society founded on freedoms of speech and association.

Congress evinced awareness of the problems with pattern-based data mining when it ended funding for the Defense Advanced Research Projects Agency (DARPA)'s Total Information Awareness (TIA) program in January, 2003.[5] TIA aimed to identify suspect patterns of behavior indicative of terrorist activity, and search personally identifiable records for such patterns, across both government and private-sector databases. The demise of TIA did not indicate the demise of data mining in the name of federal intelligence-gathering, however. In the wake of the cancellation of TIA, the

---

[3] *See generally* STEPHEN BAKER, THE NUMERATI (2008).
[4] Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. CIV. RIGHTS-CIV. LIBERTIES L. REV. 435 (2008)[hereinafter *Government Data Mining*].
[5] *Id*. at 450.

federal government provided funding to local intelligence-gathering centers with the aim of "fusing" gathered information across local and federal databases.[6] As of July 2009, the government reported seventy-two designated fusion centers around the country, twenty-seven of which employed the Homeland Security Data Network (HSDN), which "allows the federal government to move information and intelligence to the states".[7]

The natural question, of course, is what sort of legal framework might govern government data mining, both administrative and in the name of counter-terrorism.[8] The natural answer should be, but isn't, the Privacy Act of 1974.[9] This paper explores the features of the Privacy Act that let government agencies exempt themselves from the Act's otherwise admirable restrictions on the treatment of data held by the U.S. government on U.S. individuals. There are other U.S. laws that restrict data gathering and treatment by the U.S. government, such as the Electronic Communications Privacy Act (ECPA), but this paper addresses a more fundamental question: why the statute addressing the federal treatment of data held on individuals does not, in practice, address

---

[6] *See* Michael German & Jay Stanley, *What's Wrong with Fusion Centers*, ACLU, http://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf (2007) (pointing to the development of data fusing intelligence centers known as "fusion centers" around the United States, for the purpose of sharing intelligence and mining it). *See also* Joshua Rhett Miller, '*Fusion Centers' Expand Criteria to Identify Militia Members*, FOX NEWS, http://www.foxnews.com/politics/2009/03/23/fusion-centers-expand-criteria-identify-militia-members/ (Mar. 23, 2009); Department of Homeland Security Office of the Press Secretary, *Statement from U.S. Department of Homeland Security Press Secretary Sara Kuban on Secretary Napolitano's Address to the National Fusion Conference*, http://www.dhs.gov/ynews/releases/pr_1236591110719.shtm (Mar. 6, 2009) (stating that "Secretary Napolitano is committed to ensuring that all entities - federal, state, local, and tribal - are coordinating and communicating effectively" and reconfirming the existence of the DHS State, Local, and Regional Fusion Center Initiative).

[7] *State and Local Fusion Centers*, http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

[8] *Government Data Mining*, *supra* n. 6, at 437 (observing "the failure of law and the legal system to respond to the proliferation of data mining and the dramatic technological changes that make it possible").

[9] *Id*. at 465-466 (pointing out that while "[t]he broadest federal privacy law… is the Privacy Act of 1974", in reality "the Privacy Act does little to provide guidance for government data mining activities or to limit the government's power to collect personal data from third parties").

the federal treatment of data held on individuals. This paper revisits the often dismissed Privacy Act with an eye to both noting its failures and reviving its importance.

Generally, U.S. privacy law is scattered through separate statutes; the Privacy Act of 1974 represents the closest thing the United States has to omnibus federal privacy legislation.[10] The Privacy Act outlines enforceable Fair Information Practices (FIPs) for records held by agencies of the U.S. federal government. Fair Information Practices establish seven principles for the handling of data: (1) they limit the use of data; (2) they limit the collection of data; (3) they limit the disclosure of data (not always the same as data use); (4) they impose requirements for the upkeep of data, ensuring data quality; (5) they give rights to individuals, such as notice, access, and correction rights; (6) they require that data processing systems be transparent; and (7) they ensure that data will be kept securely.[11]

These principles serve the interests of both the government and individuals. Giving individuals correction rights and imposing requirements concerning the quality of information benefits the government, since incorrect information is useless. Giving individuals access rights and ensuring the transparency of process allows individuals to in turn keep tabs on the government agency that is keeping tabs on them.

The Privacy Act is founded on such principles. It circumscribes the disclosure of information, and allows individuals in some circumstances to access and correct the files the U.S. government keeps on them. The Act provides both civil remedies and criminal sanctions for lack of compliance.

---

[10] The Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31, 1974).
[11] Paul M. Schwartz, *Preemption and Privacy*, 18 Yale L.J. 902, 908 (2009) [hereinafter *Preemption and Privacy*].

Compared to the EU's Data Protection Directive, the Privacy Act is limited in scope, both in its limitation to the public sector (federal agencies) and its narrow definition of "record."[12] Compared to the rest of U.S. privacy law, however, the Privacy Act is sweeping. Most information privacy law in the United States has been sector-specific.[13] The Privacy Act on its face represents an exception to this approach; it was enacted after broader omnibus information privacy legislation was rejected by Congress, and contains significant elements of the rejected omnibus bill.[14]

On its surface, the Privacy Act appears to be a strong statement from the U.S. government regarding the treatment of records the federal government holds on its citizens. Many agencies, however, actively use structural elements of the Privacy Act to remove themselves and their records from its requirements.

The Privacy Act requires that each agency publish in the Federal Register and provide notice to Congress and the Office of Management and Budget (OMB) on proposals to establish or alter any system of records.[15] These notices, known as Systems of Records Notices (SORNs), are meant to encourage transparency in the creation of new systems of records, and alert individuals to the fact that records might be kept on them.

In actuality, the SORNs examined herein for the most part served a minimal or nonexistent transparency function—eliciting few to no comments, as few organizations or individuals appear to be monitoring them. SORNs are, instead, used by agencies to remove systems of records from the scope of the Privacy Act, through exemptions.

---

[12] Paul M. Schwartz & Joel R. Reidenberg, DATA PRIVACY LAW 92 n.4 (1996).
[13] *Id*., at 922.
[14] *Preemption and Privacy*, 18 YALE L.J. at 910 (discussing Senate Bill 3418, an omnibus bill for the private and public sectors introduced in 1974 and never enacted).
[15] 5 U.S.C. § 552a(e)(4), (o).

This paper identifies an active controversy over the scope of Privacy Act exemptions. Courts disagree over what sort of agency constitutes an agency whose "principal function" is "any activity pertaining to the enforcement of criminal laws", and what information is "information complied for the purpose of a criminal investigation".[16] Such agencies are permitted to claim the greatest exemptions from the Privacy Act; courts disagree, however, over who should be able to claim these exemptions and for what information. This question is of crucial importance when determining whether the Privacy Act governs government data mining that is tangential to law enforcement purposes, but not attached to a specific criminal investigation.

For the nonexemptable portion of the Privacy Act restricting the dissemination of records, agencies also use SORNs to broaden the scope of permissible dissemination, sometimes to the point of meaninglessness.

SORNs, in short, allow agencies to both 1) exempt systems of records from specific portions (nearly all) of the Privacy Act; and 2) expand the definition of "routine use", allowing for wide disclosure of records outside of the agency responsible for the system. From the SORNs evaluated for the purposes of this paper, it appears that this use of SORNs to expand "routine uses" and exempt agencies from Privacy Act requirements is a more recent development, overused by the Department of Homeland Security (DHS). Despite a publicly articulated privacy policy supporting Fair Information Practices, DHS uses SORNs to escape the provisions of the Privacy Act.[17]

This paper provides an overview of SORNs and how they function. Section I outlines the provisions of the Privacy Act against a larger backdrop of goals the Act

---

[16] 5 U.S.C. § 552a(j)(2).
[17] Hugo Teufel III, DHS Chief Privacy Officer, PRIVACY POLICY GUIDANCE MEMORANDUM, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

articulates. Section II examines several SORNs in detail, from DHS and, for comparative purposes, from the Department of Health and Human Services (DHHS). Section III concludes: while SORNs were intended to provide notice and transparency in the creation of new systems of records, they have come to be used by DHS in particular as loopholes in the legislation, making the practical application of the Privacy Act very different from its facial message. These agency-created exceptions are of increasing significance in an age of broad federal information-gathering and data mining for national security, emergency, and law-enforcement purposes.[18]

I. The Privacy Act: An Overview

The Privacy Act provides for a series of Fair Information Practices (FIPs) in the handling of government-controlled data on U.S. citizens. It draws on elements common to FIPs enacted in Western Europe in the 1970s: (1) limits on information use; (2) limits on data collection, or "data minimilization"; (3) limits on disclosure of personal information; (4) requirements for data quality; (5) notice, access, and correction rights for the individual; (6) requirements for transparent processing systems; and (7) security of personal data.[19] These practices are bolstered by civil remedies and criminal sanctions for failure to comply. This Section outlines the requirements of the Privacy Act, the sanctions that enforce those requirements, and finally, the exemptions and exceptions the Privacy Act allows for in its text.

a. Privacy Act Requirements

---

[18] *See generally* note 6.
[19] Paul M. Schwartz, *Preemption and Privacy*, 18 Yale L.J. 902, 908 (2009) [hereinafter *Preemption and Privacy*].

The Privacy Act governs the treatment of "any record which is contained in a system of records" on a "citizen of the United States or an alien lawfully admitted for permanent residence" by an agency of the federal government.[20] The Privacy Act imposes essentially two types of requirements: 1) requirements concerning government treatment of records (their use, distribution, and maintenance), and 2) requirements concerning individuals' access to the data kept on them. The first set of requirements governs how information is collected, maintained, disclosed, and/or circulated.[21] The second allows individuals to contact agencies and request to see the files held on them, and provide corrections if necessary.[22] Generally speaking, the latter half of requirements regarding access to individual records, known as first person access rights, does not apply when an individual attempts to gather information pertaining to a law enforcement investigation, criminal or civil, about that individual.

The Privacy Act imposes requirements regarding the collection of information about an individual. It requires that when an agency uses its records to determine an individual's "rights, benefits, and privileges under Federal programs", it must "to the greatest extent practicable" collect information about an individual "directly from the subject individual".[23] The information collected, regardless of whether benefits are dependent on it, must be limited to that which is "relevant and necessary to accomplish a purpose of the agency required… by statute or by executive order of the President".[24] The

[20] 5 U.S.C. § 552a (a)(1), (a)(2), (b), (m)(1) (this includes government contractors that "accomplish an agency function").
[21] 5 U.S.C. § 552a (b), (c), (e).
[22] 5 U.S.C. § 552a (d), (f).
[23] 5 U.S.C. § 552a (e)(2).
[24] 5 U.S.C. § 552a(e)(1).

agency must satisfy a number of notice requirements before a system of records can be maintained, including the publication of a SORN.[25]

The core of the Privacy Act is as follows: once information is in a system of records, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains".[26] This is strong language. Information in a federal system of records may not be disclosed to any person, or to any other agency, unless the individual implicated by the record requests or consents to that distribution.

There are, however, exceptions to this apparently clear-cut rule, even within the Privacy Act itself. These exceptions include: disclosure to officers and employees of the agency that retains the records, disclosure for statistical research, disclosure to the Bureau of the Census, disclosure to the National Archives and Records Administration, disclosure to another agency pursuant to a written request by the head of that agency "for a civil or criminal law enforcement activity if the activity is authorized by law", and disclosure to consumer reporting agencies.[27]

Most significant of the dissemination exceptions mentioned in the Act, however, is disclosure for "a routine use", which allows agencies leeway in controlling the scope of dissemination of the information through SORNs.[28] Agencies use the "routine use" exception to nondisclosure requirements to vastly expand their disclosure abilities beyond the exceptions articulated in the Privacy Act itself.

---

[25] 5 U.S.C. § 552a(e), (o).
[26] 5 U.S.C. § 552a(b).
[27] 5 U.S.C. § 552a(b)(1)-(12).
[28] 5 U.S.C. § 552a(b)(3), (a)(7).

The second prong of the Privacy Act allows individuals to request access and amendments to records held on them.[29] Again, on its face the Act is stringent in its requirements: "upon request" the agency must allow an individual "to review the record and have a copy made of all or any portion thereof in a form comprehensible to him".[30] The agency must also "promptly" make any corrections or deletions the individual requests, provide reasons for not making said amendments, and provide a system of review for decisions not to amend.[31] Many agencies, however, exempt themselves from the access requirements of the Act under the general exemptions of subsection (j)(2), or specific exemptions of (k)(2).

b. Privacy Act Sanctions

The Privacy Act provides both civil and criminal sanctions, which apply to different subsections.

The Act provides that an individual may bring a civil action in district court against an agency whenever 1) the agency does not amend that individual's record according to his or her request, or fails to review the record; 2) the agency refuses to allow an individual access to his or her records; 3) an adverse determination of benefits is made on the basis of an improperly maintained record; or 4) more vaguely, the agency fails to comply with the Act and that failure has an "adverse effect" on the individual.[32] The court determines the matter of amendment of agency records de novo, and may order the specific performance of amending the records. For an adverse determination of benefits or "adverse effects" on the individual, when the agency behavior is willful or

[29] 5 U.S.C. § 552a(d).
[30] 5 U.S.C. § 552a(d)(1).
[31] 5 U.S.C. § 552a(d).
[32] 5 U.S.C. § 552a(g)(1).

intentional, the Act includes a minimum damage of $1,000 and an award of actual damages to the individual.[33]

The Act also provides for criminal penalties for three different activities. The first criminal provision outlines a misdemeanor with a maximum $5,000 fine for the willful disclosure by an officer or agency employee of agency records containing individually identifiable information, with the knowledge that disclosure of such material is prohibited, to any person or agency not entitled to receive it.[34] The second misdemeanor, also carrying a maximum fine of $5,000, applies to officers or agency employees who willfully forego the notice requirements by failing to publish a SORN.[35] The third misdemeanor, carrying the maximum fine of $5,000, targets any person who knowingly and willfully requests and obtains an agency record concerning an individual under false pretenses.[36]

c. Privacy Act Exemptions and the "Routine Use" Exception

The Privacy Act contains a list of acceptable disclosures, plus two types of exemptions. Acceptable disclosures include disclosure within the agency, disclosure to the public under the Freedom of Information Act, disclosure for statistical research, and disclosure for law enforcement purposes if the head of the agency making the request has made a written request "specifying the portion desired and the law enforcement activity for which the record is sought".[37] These acceptable disclosures also, however, include

[33] 5 U.S.C. §552a(g)(4)(A).
[34] 5 U.S.C. § 552a(i)(1).
[35] 5 U.S.C. §552a(i)(2).
[36] 5 U.S.C. § 552a(i)(3).
[37] 5 U.S.C. § 552a(b)(7).

any additional "routine use" that an agency has established and described in a SORN under (e)(4)(D).[38]

i. Routine Use: A loophole for dissemination restrictions

Routine use exceptions are used by agencies to expand permissible dissemination from the facial restrictions of the Privacy Act.[39] Using a routine use exception to create new dissemination standards can effectively remove an agency from the core non-dissemination principles of the statute, including criminal sanctions for employees who improperly disclose information to individuals or agencies outside of the agency.[40] If disclosure is practically so broad as to never be improper, then there can be no sanctions for improper disclosure.

"Routine use" is defined as "the use of such a record for a purpose which is compatible with the purpose for which it was collected."[41] The Privacy Act Guidelines of July 9, 1975[42] clarify this tautology by explaining that "routine use" is not dependent on frequency of use: it is meant to include both "the common and ordinary uses to which records are put" and "all of the proper and necessary uses even if such use occurs

---

[38] 5 U.S.C. § 552a(b)(3), (a)(7).

[39] Several authors have recognized the expansive nature of routine uses, but none have performed categorical or comparative analysis of what they do in SORNs. *See, e.g.*, Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279 (2010) (only briefly noting the routine use exception but not observing its scope in practice); Dennis J. McMahon, Comment, *The Future Of Privacy In A Unified National Health Information Infrastructure*, 38 SETON HALL L. REV. 787, 797 (2008) (discussing the routine use exception in the context of health information as the "most glaring loophole", but not observing how it operates in practice); Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. CIV. RIGHTS-CIV. LIBERTIES L. REV. 435 (2008)(noting the routine use exemption); Jonathan C. Bond, *Defining Disclosure in a Digital Age: Updating the Privacy Act for the Twenty-First Century*, 76 GEO. WASH. L. REV. 1232 (2008) (explaining the administrative process and use of routine uses, but again not providing examples or discussing the potential or actual scope, and concluding that routine use exceptions are not problematic); James McCain, *Applying the Privacy Act of 1974 to Data Brokers Contracting With the Government*, 38 PUB. CONT. L.J. 935 (2009) (noting the expansive properties of the routine use exception, but not providing concrete examples).

[40] 5 U.S.C. § 552a(i)(1).

[41] 5 U.S.C. §552a(a)(7).

[42] Privacy Act Guidelines, 40 Fed.Reg. 28949, 28961 (July 9, 1975) [hereinafter Privacy Act Guidelines].

infrequently."[43] The term more appropriately applies to uses that are "not only compatible with, but related to, the purpose for which the record is maintained".[44]

The Privacy Act Guidelines point to two examples of routine uses "applicable to a substantial number of systems of records but which are only permissible if properly established by each agency".[45] These include 1) disclosures to law enforcement when criminal misconduct is suspected in connection with the administration of a benefits program; and 2) disclosures to an investigative agency for a background check. Agencies now use SORNs to establish many other forms of routine use.

ii. Exemptions: Getting out of the Privacy Act

The Privacy Act provides for two types of exemptions from the majority of its terms: general exemptions and specific exemptions.[46] General exemptions allow the head of an agency to exempt a system of records within the agency from a large number of the subsections of the Privacy Act. General exemptions apply only, however, to a system of records maintained by 1) the CIA, or 2) "an agency… which performs as its principal function any activity pertaining to the enforcement of criminal laws" and which system of records contains records addressing either the identification information for individual criminal offenders, records "compiled for the purpose of a criminal investigation", or records generated on an individual in law enforcement custody.[47] Specific exemptions, which are substantially narrower than general exemptions, may be claimed by any agency—not just an agency or subagency specializing in criminal law enforcement—for

[43] *Id*. at 28953.
[44] *Id*.
[45] *Id*.
[46] 5 U.S.C. §552a(j), (k).
[47] 5 U.S.C. §552a(j)(2).

systems of records comprising "investigatory material compiled for law enforcement purposes", plus five other narrower categories.[48]

The scope of general exemptions is wide. General exemptions allow an agency, with appropriate notice, to exempt the applicable system of records from every subsection of the Privacy Act except the following: (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i). General exemptions still must be claimed one-by-one, and the claiming agency must explain "the reasons why the system of records is to be exempted from a provision of this section."[49] Recent SORNs, however, have tended to claim all possible general exemptions if the agency believes it qualifies for them.

In more comprehensible terms, general exemptions retain only the following portions of the Privacy Act: terms limiting disclosure and dissemination of records; the requirement of accurate accounting of disclosures; notice requirements requiring SORN publication in the Federal Register; a requirement that the agency make reasonable efforts to assure records are "accurate, complete, timely, and relevant for agency purposes" before disseminating to any person other than an agency; a requirement that the agency maintain no records of the exercise of First Amendment rights unless pertinent to an authorized law enforcement activity; rules of conduct for persons handling the records; technical and physical safeguards to insure security and confidentiality of the records; and all criminal penalties.

If an agency claims all of the possible general exemptions, all individual access-to-data rights are eliminated, all data amendment and correction rights are eliminated,

[48] 5 U.S.C. § 552a(k)(2).
[49] 5 U.S.C. 552a(j).

basic data quality requirements are eliminated, and civil remedies are eliminated.[50] If an agency invokes all general exemptions of the Privacy Act, the Act is effectively limited to governing dissemination and protection of data. As mentioned above, however, the governance of dissemination is severely weakened by the overexpansion of "routine use" in SORNs. The combination of a full claim of general exemptions plus expansive routine use effectively takes an agency outside of the Privacy Act entirely.

Specific exemptions are significantly narrower. Rather than specifying which subsections of the act remain in existence, specific exemptions limit exemptions to subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f). An agency may exempt a system of records from any or all of those subsections if that system of records falls in any of the following categories: investigatory material compiled for law enforcement purposes; material maintained in connection with providing protective services to the U.S. President; statistical records; investigatory material for determining qualifications for Federal employment, military service, Federal contracts, or access to classified information; testing material that would compromise the fairness of the testing process; and evaluation material for promotion in the armed services.[51] Several of these exemptions are further limited to material that would reveal the identity of a source who has explicitly been granted confidentiality.[52]

Specific exemptions allow an agency to exclude itself from only the following Privacy Act subsections: the access-to-records requirement; the requirement that the

---

[50] Courts disagree on this point. At least one court has held that general exemptions do not allow agencies to exempt themselves from civil remedies, finding that liability is not an exemptable portion of the act. *Tijerina v. Walters*, 821 F.2d 789 (D.C. Cir. 1987). At least two other courts have, however, established in dicta that general exemptions do include the elimination of civil sanctions. *Kimberlin v. Dept. of Justice*, 788 F.2d 434, 436 n. 2 (7th Cir.1986); *Ryan v. Dept. of Justice*, 595 F.2d 954, 958 (4th Cir.1979).
[51] 5 U.S.C. § 552a(k).
[52] 5 U.S.C. §552a(k)(2).

agency provide lists of any disclosures to an individual upon request; the requirement that an agency "maintain in its records only such information… as is relevant and necessary to accomplish a purpose of the agency"; the notice requirement concerning the category of records in the system; and agency rules and procedures for access.[53] Specific exemptions, then, provide a lesser opt-out that deals primarily with access requirements.

Specific exemptions, unlike general exemptions, do not allow an agency to opt out of the requirement that the agency "maintain all records… used… in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[54] Specific exemptions also do not allow the agency to opt out of civil remedies for failing "to comply … in such a way as to have an adverse effect on an individual".[55] Thus, specific exemptions maintain both data quality requirements and supporting sanctions that general exemptions do not provide.

iii. Criminal Law Enforcement and General Exemptions

As discussed, general exemptions allow an agency to opt out of more of the Privacy Act than specific exemptions do. General exemptions are meant to apply, however, to only a very specific type of agency and record. Significant disagreement exists on whether general exemptions should apply to all records held by criminal law enforcement agencies, or to only those records tied to a specific criminal investigation. This section aims to more clearly define when general exemptions should apply.

The Privacy Act establishes that general exemptions apply only in limited circumstances, as follows:

---

[53] 5 U.S.C. § 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f).
[54] 5 U.S.C. 552a(e)(5).
[55] 5 U.S.C. § 552a(g)(1)(D).

> The head of any agency may promulgate rules…to exempt any system of records within the agency… if the system of records is…(2) maintained by an agency or component thereof which performs as its *principal function any activity pertaining to the enforcement of criminal laws…and* which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) *information compiled for the purpose of a criminal investigation*, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.[56]

This language has fostered disagreement between subsets of representatives, academics, and courts, who roughly split between two views: 1) subsection (j)(2) means that a criminal law enforcement agency may exempt any of its records from most of the Privacy Act, or 2) a criminal law enforcement agency may exempt only those records more narrowly "compiled for the purpose of a criminal investigation".

The first, and in my view incorrect, interpretation reads (j)(2) as exempting all records belonging to a criminal law enforcement agency. The Privacy Act Guidelines do not provide deep interpretation of (j)(2) but assert in passing that (j)(2) is a broad exemption covering all "records maintained by an agency whose principal function pertains to the enforcement of criminal laws".[57] This view is not unsupported, despite its apparent inconsistency with the text of the Privacy Act. Writing about the Privacy Act in 1975, James H. Davidson argued that the general exemptions followed the House, rather than the Senate, version of the bill. "The Senate bill would have permitted exemptions only for certain law enforcement investigative and intelligence files. The broader exemption for systems of records maintained by any agency or component whose

[56] 5 U.S.C. § 552a(j)(2)(emphases added).
[57] Privacy Act Guidelines, *supra* note 33.

principal function pertains to criminal law enforcement was accepted in deference to still active efforts in both the House and Senate to pass criminal justice information legislation."[58] In fact, debates continued on such criminal justice information legislation after the Privacy Act was passed, but ultimately fizzled out.

This view—that a criminal law enforcement agency's records are exempted by (j)(2), regardless of the type of record—was taken up by others, as well. Another contemporaneous writer observed that "[e]xemptions can be invoked for the records of the CIA, [and] criminal law enforcement agencies".[59] Davidson pointed out that the process of rulemaking, not the text of the Act, was meant to serve as a check on criminal law enforcement agencies. "By requiring open rule making with the receipt of comments and an agency statement explaining the exception for certain categories of records, the Congress was trying to avoid creation of a loophole which would permit entire agencies to avoid compliance with the Act."[60]

Several courts have followed this interpretation, exempting systems of records solely because they are held by an agency whose primary purpose is criminal law enforcement. A Pennsylvania court found that "(j)(2) permits an agency head to promulgate rules that allows the agency to withhold information if that agency 'performs as its principal function any activity pertaining to the enforcement of criminal laws…'".[61] Similarly, a District Court in the Southern District of New York found that "the Privacy Act expressly exempts from its access and challenge provisions, the records of any

---

[58] Davidson *Privacy Act*, *supra* note 1. *Available in* Legislative History of the Privacy Act of 1974, Source Book on Privacy, 1191, 1194 (1976) [hereinafter Source Book on Privacy].
[59] Mary Hulett, *Privacy and the Freedom of Information Act*, 27 Admin. L. Rev. 275, 287 (1975).
[60] *Id*. at 1193.
[61] *Amro v. U.S. Customs Service*, 128 F.Supp.2d 776, 782 n. 8 (E.D. Pa. 2001).

agency whose 'principal function' pertains to the 'enforcement of criminal laws…'".[62] The New York court did refer in passing to the facial record-type requirement, but made it a very loose requirement indeed; to qualify for general exemption (j)(2), it was sufficient for the agency to show that it "is such a… [criminal law enforcement] agency, and that records sought by plaintiff related to [its] law enforcement activities".[63] Two recent D.C. cases have echoed this reasoning, contrary to strong D.C. precedent requiring tailoring to a specific criminal investigation.[64]

For this reading—that any records held by a criminal law enforcement agency are exemptable under (j)(2)—to be consistent with the record-type requirements on the face of (j)(2), one must understand the types of records outlined in (j)(2) as effectively describing all records held by a criminal law enforcement agency. As one contemporaneous article describes it, "[s]ubsection (j)(2) allows criminal law enforcement agencies to exempt certain types of records that they maintain".[65] However, in this understanding of (j)(2), those "certain types" are not limiting, but expansive: "[t]his list seems to encompass all records held for criminal law enforcement purposes."[66]

This reading away of the type-of-records requirements of (j)(2) is incorrect. The other reading of (j)(2)—that the Privacy Act limits general exemptions to only *specific types of records* held by criminal law enforcement agencies—finds significant support

---

[62] *Nunez v. Drug Enforcement Administration*, 497 F.Supp. 209, 211 (S.D.N.Y. 1980).
[63] *Id*.
[64] *See Willis v. U.S. Dept. of Justice*, 581 F.Supp.2d 57, 77 (D.D.C. 2008)(reasoning that "(j)(2) of the Privacy Act exempts from mandatory disclosure systems of records 'maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws…'" and "the records concerning Plaintiff were compiled pursuant to numerous activities pertaining to the enforcement of criminal laws, and were therefore exempt"); *Dorsett v. U.S. Dept. of Treasury,* 307 F.Supp.2d 28, 35 (D.D.C. 2004)(reasoning that "(j)(2) exempts from disclosure 'any system of records within the agency,' as long as the agency that maintains the system of records 'performs as its principal function any activity pertaining to the enforcement of criminal laws....'").
[65] Excerpts from *Increasing Protection of Citizen Privacy*, 73 MICH. L. REV. 1221, 1332 (1975), *available in* Source Book on Privacy, *supra* note 49 at 1364.
[66] *Id*. at 1333, 1365

both in the text of the statute itself, in contemporaneous understandings, and in crystal clear court opinions.

First, reading (j)(2) as encompassing *all* records of an agency whose principal purpose is criminal law enforcement constitutes a misreading far broader than (j)(2)'s facial requirements. Subsection (j)(2) on its face requires both an agency type (criminal law enforcement) and a type of record, limited to "a criminal investigation" or arrest records or reports identifiable to an individual from arrest to conviction. For a system of records to be subject to general exemptions, then, two requirements must be satisfied: 1) the principal function of the agency or agency's component must be criminal law enforcement, and 2) the records themselves must be related to an arrested or jailed individual, or be "for the purpose of a criminal investigation".[67] This suggests that a concrete, tailored investigation must exist for records to be subject to general exemptions. If an agency whose principal function is criminal law enforcement collects broad surveillance information about an individual that is not "for the purpose of a criminal investigation", that information should not be subject to general exemptions of the Privacy Act.

This analysis is further supported by language in other portions of the Privacy Act. One example is the narrowness of the exemption from the Act's restrictions on matching programs for matches performed by criminal law enforcement agencies only "subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons".[68] This exempts only such queries as are connected to a specific open

[67] 5 U.S.C. §552a(j)(2).
[68] 5 U.S.C. § 552a(a)(8)(B)(iii).

investigation. While the general exemption language is not as limited as this language on matching program restrictions, (j)(2)'s use of the term "the purpose of a criminal investigation" instead of "criminal investigating" or "criminal law enforcement" similarly indicates that an actual investigation must exist for general exemptions to be claimed. Another feature of the Privacy Act that points to the narrowness of (j)(2) is the language of (k)(2), which does not limit "investigatory material compiled for law enforcement purposes" to civil law enforcement, but encompasses all material not covered by (j)(2). This lack of specificity suggests that (j)(2) is meant to encompass other types of criminal law enforcement records that aren't covered by (j)(2)'s specific record requirements.

Despite their assertion that (j)(2) applies to all criminal law enforcement agency records, the Privacy Act Guidelines do point to important contextual information for interpreting the (k)(2) phrase "investigatory material compiled for law enforcement purposes" which confirms that *both* (j)(2) and (k)(2)'s scope should be limited to actual investigations, not surveillance or pattern-based data mining of the general public for suspect individuals. The Privacy Act Guidelines highlight the importance of the existence of "an investigation of an alleged or suspected violation of civil laws".[69] The Guidelines further state that the case law interpreting "investigatory" and "law enforcement purposes" for exemption (b)(7) of the Freedom of Information Act (FOIA) "should be utilized in defining these terms as they appear in subsection (k)(2) of the Privacy Act".[70]

To show that records are "compiled for law enforcement purposes" under FOIA, an agency whose primary purpose is not criminal law enforcement must show that the

[69] Privacy Act Guidelines, *supra* note 33 at 28972.
[70] *Id*. at 28973.

records involved the enforcement of a statute or regulation within its authority,[71] and were compiled for "adjudicative or enforcement purposes".[72] Furthermore, use of the term "investigatory" in subsection (k)(2) specifically limits included records to "investigatory records that are compiled in the course of a specific investigation".[73] In the case of subsection (j)(2), which addresses criminal law enforcement, corresponding FOIA cases have given greater deference to criminal law enforcement agencies. Some courts have held that records of criminal law enforcement agencies are per se compiled for law enforcement purposes.[74] Others, however, have required even criminal law enforcement agencies to show a nexus between records and a proper law enforcement purpose.[75] Furthermore, if an agency compiles records outside of its law enforcement authority, those records may not be withheld under FOIA.[76]

The inclusion of the terms "for the purpose of a criminal investigation" in (j)(2) suggests an even narrower scope than "compiled for law enforcement purposes" language of FOIA (b)(7); therefore, (j)(2) limits general exemptions to material related to existing criminal investigations (plus the smaller categories of (A) identifying information and notations of arrest and sentencing, and (C) reports compiled during the process of enforcement, from arrest through release).

Courts, when considering general exemptions more thoroughly, have concluded that this is the correct interpretation of (j)(2): it is limited to specific types of records

---

[71] *Lewis v. I.R.S.*, 823 F.2d 375 (9th Cir. 1987).
[72] *Rural Housing Alliance v. U.S. Dept. of Agriculture*, 498 F.2d 73 (D.C. Cir. 1974), opinion supplemented, 511 F.2d 1347 (D.C. Cir. 1974).
[73] *Cox v. U.s. Dept. of Justice*, 576 F.2d 1302, 1310 (8th Cir. 1978).
[74] *Williams v. F.B.I.*, 730 F.2d 882 (2d Cir. 1984); *Curran v. Department of Justice*, 813 F.2d 472 (1st Cir. 1987); *Ferguson v. F.B.I.*, 957 F.2d 1059 (2d Cir. 1992).
[75] *Pratt v. Webster*, 673 F.2d 408 (D.C. Cir. 1982).
[76] *Weissman v. Central Intelligence Agency*, 565 F.2d 692 (D.C. Cir. 1977) (CIA may not conduct domestic law enforcement, therefore records of investigating American citizens in the United States are not protected).

pertaining to concrete criminal investigations, not broadly applicable to all records held by a criminal law enforcement agency. The Court of Appeals for the D.C. Circuit has been the most articulate on this line of reasoning. In Vymetalik v. F.B.I., the court held that the F.B.I. not only could not rely on (j)(2), but also could not use (k)(2) to claim specific exemptions from the Privacy Act for materials compiled during F.B.I. security checks on an individual. Citing Pratt v. Webster, the court reasoned that "FBI records are not law enforcement records simply by virtue of the function that the FBI serves…[i]nstead, the characterization of the records at issue turns upon the type of investigation involved."[77] The court concluded that "[i]f specific allegations of illegal activities were involved, then this investigation might well be characterized as a law enforcement investigation. Should the FBI come forward with evidence suggesting a law enforcement purpose other than mere background investigation, the District Court remains free to conclude that the records constitute law enforcement records."[78]

Several cases both in D.C. and elsewhere have followed Vymetalik's reasoning and concluded that for records to be "for the purpose of a criminal investigation"(j)(2) or more broadly "investigatory material compiled for law enforcement purposes"(k)(2), an actual specific investigation in some way implicating the individual must exist. In Doe v. F.B.I., the D.C. Court of Appeals held that (j)(2)(B) "authorizes a law enforcement agency to exempt any system of records consisting of 'information compiled for the purpose of a criminal investigation ... and associated with an identifiable individual'".[79] In critical language, the court held that "[a]n agency does not satisfy this requirement when 'merely engaging in a general monitoring of private individuals' activities'; rather,

[77] Vymetalik v. F.B.I., 785 F.2d 1090, 1095 (C.A.D.C. 1986)(citing Pratt, 673 F.2d at 420-421).
[78] *Id*. at 1098.
[79] *Doe v. F.B.I.*, 936 F.2d 1346, 1351 (C.A.D.C. 1991).

the agency must demonstrate a connection between its investigation and the existence of a 'possible security risk or violation of federal law.'"[80]

An Illinois court and New Jersey Court have both followed similar reasoning. In Illinois, the court found that an agency must meet three requirements to qualify for general exemptions under (j)(2): "show that it is engaged primarily in law enforcement activities, that the records to be exempted were compiled for the purpose of criminal investigation, and that it has promulgated rules exempting the system of records from disclosure and stating its reasons for the exemption."[81] Lest one confuse "for the purpose of criminal investigation" with a wider mandate of criminal law enforcement, the court exempts records that were "all…compiled in the course of investigations into [plaintiff's] criminal activities."[82] The New Jersey court more forcefully distinguished between records compiled for the purpose of a criminal investigation, and records compiled by a criminal law enforcement agency. The court held that "[t]he FBI cannot claim that all of its records must necessarily be considered as compiled for purposes of criminal investigation merely by virtue of the function that the FBI serves… Instead, the FBI must adequately demonstrate that its records on plaintiff were compiled specifically for purposes of a criminal investigation."[83]

Therefore, systems of records held by criminal law enforcement agencies that do not pertain to concrete criminal investigations should be subject instead to specific exemptions, or—depending on whether they pertain to any law enforcement investigation and how narrowly one reads the requirements of (k)(2)—no exemptions at all.

---

[80] *Id*. at 1353 (citing *Pratt*, 673 F.2d at 420; cf. *Shaw v. FBI*, 749 F.2d 58, 64-65 (D.C.Cir.1984) (Scalia, J.) (exemption extends to investigation, conducted for "federally authorized purpose," of non-federal crime)).
[81] *Stimac v. F.B.I.*, 577 F.Supp. 923, 925 (D.C.Ill.,1984).
[82] *Id*.
[83] *Patterson v. F.B.I.*, 705 F.Supp. 1033, 1042-1043 (D.N.J.,1989).

Again, specific exemptions require that while the agency may exempt the records from the access provisions of the Act, an agency must retain both civil sanctions and at least the maintenance requirements of (e)(5), requiring relevancy, accuracy, and timeliness for information based on which adverse determinations are made. This ensures higher quality data, and enforcement provisions that benefit any individuals harmed by agency misbehavior.

II. System of Records Notices (SORNs): Agency tools for opting out

System of Records Notices, or SORNs, are ostensibly meant to serve a transparency function by alerting individuals to the existence of systems of records held on them. SORNs are governed by notice-and-comment rulemaking.[84] SORNs inform individuals through publication in the Federal Register of the system name, location, maintenance, security policies, and other features.[85] SORNs also, however, allow agencies to carve themselves out of the Privacy Act through 1) expansive articulations of "routine use" of the records, and 2) claiming exemptions to the Privacy Act under Sections (j) and (k).

This section examines SORNs from the Department of Homeland Security (DHS) and the Department of Health and Human Services (DHHS). The scope of the SORNs differs considerably depending on the agency articulating them. This section finds that DHS subagencies use SORNs to effectively opt out of the Privacy Act, by classifying themselves as criminal law enforcement agencies, invoking all exemptions available under general exemptions, and broadening the "routine uses" available to them until there are few to no dissemination restrictions on the information they hold. DHHS agencies, on

[84] 5 U.S.C. § 552a(v)(1).
[85] 5 U.S.C. § 552a(2)(4).

the other hand, rarely invoke Privacy Act exemptions, and instead use routine use exceptions to broaden the permissible scope of dissemination. The routine use exceptions invoked by DHHS are significantly narrower, however, than those invoked by DHS.

a. DHS SORNs

This paper examines five SORNs from subagencies under the Department of Homeland Security (DHS): two from the U.S. Secret Service, one from Immigration and Customs Enforcement (ICE), one from the Federal Emergency Management Agency (FEMA), and one from Customs and Border Protection (CBP).[86] Despite the fact that these systems of records are controlled by different subagencies, the language of the SORNs in all but one is nearly identical, indicating that DHS has a single form it uses across subagencies for claiming Privacy Act exemptions. This is legally problematic if one believes that the standard for meeting general exemptions is high, and applies to only a subcategory of criminal law enforcement records. It is unclear that every system of records for which DHS has claimed general exemptions in fact meets the general exemption standard of being from an agency whose "principal function" is "any activity pertaining to the enforcement of criminal laws", and which information is "information complied for the purpose of a criminal investigation".[87]

The DHS SORNs serve a minimum transparency function. Of the five examined, two received no comments, one received six comments, and one provided only one

[86] U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 Fed. Reg. 43650-02 (Aug. 6, 2007), 2007 WL 2227240 (F.R.) (2007); Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection (ICEPIC) System, System of Records, 73 Fed. Reg. 48117-01 (Aug. 18, 2008), 2008 WL 3821244 (F.R.) (2008); Federal Emergency Management Agency, National Emergency Family Registry and Locator System System of Records, 74 Fed. Reg. 48767-01 (Sep. 24, 2009), 2009 WL 3028107 (F.R.) (2009); U.S. Secret Service Non-Criminal Investigation Information System of Records, 74 Fed. Reg. 45088-01 (Aug. 31, 2009), 2009 WL 2703831 (F.R.) (2009); U.S. Secret Service Criminal Investigation Information System, 74 Fed. Reg. 45087-01 (Aug. 31, 2009), 2009 WL 2703830 (F.R.) (2009).

[87] 5 U.S.C. § 552a(j)(2).

month for comments (and it is unclear how many were submitted). One of the five SORNs examined received a strikingly unusual 641 comments[88]; on further research, it became clear that the Electronic Frontier Foundation had widely publicized the issuance of this SORN, which became a cause for privacy activists. The other SORNs, however, elicited little or no response, or provided meaningless time for comments.[89]

i. DHS Exemptions: Elimination of Privacy Act requirements, except restrictions on dissemination

The DHS subagencies examined herein use SORNs to opt out of the Privacy Act with the largest possible number of exemptions under the general exemptions category. Remember that even though an agency may qualify for a general exemption, they must still individually justify their reasons for claiming each of the exemptions. These DHS subagencies also, however, redundantly claim specific exemptions, even though these overlap with the general exemptions claimed.

The five DHS SORNs examined apply to a variety of records kept by a variety of subagencies. With one exception, the SORNs are all nearly identical in the exemptions and routine uses claimed. This paper examines SORNs from the following DHS systems of records: the U.S. Customs and Border Protection (CBP) Automated Targeting System (ATS); Immigration and Customs Enforcement (ICE)'s Pattern Analysis and Information Collection (ICEPIC) System; Federal Emergency Management Agency (FEMA)'s National Emergency Family Registry and Locator System; the U.S. Secret Service's

---

[88] U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 Fed. Reg. 43650-02 (Aug. 6, 2007), 2007 WL 2227240 (F.R.) (2007) [hereinafter CBP ATS SORN].

[89] The FEMA SORN provided only one month for comments. Federal Emergency Management Agency, National Emergency Family Registry and Locator System System of Records, 74 Fed. Reg. 48767-01 (Sep. 24, 2009), 2009 WL 3028107 (F.R.) (2009) [hereinafter FEMA NEFR SORN].

Non-Criminal Investigation Information System of Records; and the U.S. Secret Service's Criminal Investigation Information System.

These systems of records differ in function. The CBP Automated Targeting System (ATS) is "an enforcement screening tool" that "compares traveler, cargo, and conveyance information against intelligence and other enforcement data" whenever "travelers or goods seek to enter, exit, or transit through the United States."[90] ICE's Pattern Analysis and Information Collection System (ICEPIC) analyzes DHS records concerning immigrants, nonimmigrants, and U.S. Citizens and LPRs, and looks for "non-obvious relationship patterns among individuals and organizations that are indicative of violations of the customs and immigration laws".[91] FEMA's National Emergency Family Registry and Locator System allows individuals displaced by national emergencies to voluntarily register themselves and give their location and other personal information so family members may find them. The U.S. Secret Service's Criminal Investigation System of Records collects information on Secret Service criminal investigations, and the Non-Criminal Investigation System of Records collects information about non-criminal Secret Service investigations.

Of the five DHS SORNs examined, four of them—all except FEMA—claimed all exemptions available as general exemptions under 5 U.S.C. §552a(j)(2) as "an agency… which performs as its principal function any activity pertaining to the enforcement of criminal laws". These SORNs claiming general exemptions exempt the respective systems from (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5),

[90] CBP ATS SORN, *supra* note 78.
[91] Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection (ICEPIC) System, System of Records, 73 Fed. Reg. 48117-01 (Aug. 18, 2008), 2008 WL 3821244 (F.R.) (2008) [hereinafter ICEPIC SORN 1].

(e)(8), (f), and (g). Translated into real language, these exemptions are from the following Privacy Act subsections: accounting for unauthorized disclosures to individuals on whom records are kept; allowing individuals access to records; maintaining only information that is relevant and necessary; collecting information directly from individuals to whom it pertains; giving notice to individuals when they are providing information; agency requirements for granting access; maintenance of information used in making any determination; serving notice on individuals when information is made available to somebody else; and civil remedies.

Effectively, what remains in this gutted version of the Privacy Act is the following: restrictions on disclosure, requirements that the agency keep an account of disclosures, assurances of the security and confidentiality of records, and criminal penalties.

It is not surprising that DHS does not want individuals to be able to access or amend their records. However, the claimed exemptions go further than limiting access or ensuring that criminals are not alerted to pending investigations or the identity of confidential sources. They also include maintenance requirements that more directly implicate the quality of the data being kept.

There are two maintenance provisions from which subagencies are exempted by most DHS SORNs: (e)(1) and (e)(5). The first, (e)(1), requires that an agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President". The second, (e)(5), requires the agency to "maintain all records which are used by the agency in making any determination about any individual

with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination".

The first of these provisions, (e)(1), imposes an important limit on the kind and amount of information gathered and maintained on an individual by restricting it to what is "relevant and necessary" to the agency's statutory purpose. As explained in the Privacy Act Guidelines, this provision supports the "key objective of the Act… to reduce the amount of personal information collected by Federal agencies to reduce the risk of intentionally or inadvertently improper use of personal data."[92] This subsection serves a narrowing function important to the principles of the Act; "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[93] Subsection (e)(1) requires an agency to "review the nature of the information which they maintain", and information maintained cannot just be "relevant; it must be both relevant and necessary."

DHS justifies its claim to exempting itself from (e)(1) by explaining that "in the course of investigations into potential violations of Federal law… the accuracy of information obtained… occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation".[94] DHS further explains that "in the interests of protective law enforcement… it is appropriate to retain all information that may aid in establishing patterns of unlawful activity".[95]

This type of law enforcement pattern-searching is outside of the conceived scope of the Privacy Act, and may create as many problems as it solves. More data creates more

---

[92] Privacy Act Guidelines, *supra* note 33, at 28960.
[93] *Id*.
[94] U.S. Secret Service Criminal Investigation Information System, 74 Fed. Reg. 45087-01 (Aug. 31, 2009), 2009 WL 2703830 (F.R.) (2009) [hereinafter U.S. Secret Service Criminal SORN].
[95] *Id*.

noise, and more patterns to choose from; it doesn't just point to a clear answer to mysteries.[96] The "relevancy and necessity" requirement is thus potentially as helpful for the agency as for the U.S. citizens it protects. It should not be hard to show that all information gathered on an individual in the course of a criminal investigation is "relevant and necessary" to that investigation; however, it should be hard to show that information gathered about U.S. citizens not associated with a criminal investigation is relevant and necessary to the agency's purpose.

The second maintenance exemption, (e)(5), concerns an even more fundamental requirement, one that appears to minimally impinge on an agency's flexibility. When making a determination regarding an individual, the agency must maintain records with such "accuracy, relevance, timeliness and completeness" as is "reasonably necessary" to assure fairness to that individual. DHS again explains that "in the collection of information for law enforcement and protective purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance… would preclude Secret Service DHS agents from using their investigative and protecting training and exercising good judgment to both conduct and report on investigations or other protective activities".[97]

First, this reasoning is a misinterpretation of the requirement of (e)(5). Subsection (e)(5) does not mandate that information entering the system must be accurate, relevant, timely, and complete. The provision instead mandates that agency determinations be

---

[96] Ed Felten, *Needle-in-a-Haystack Problems*, Freedom to Tinker, Apr. 23, 2010, http://www.freedom-to-tinker.com/blog/felten/needle-haystack-problems (observing that for problems with "big haystacks", where the right answer is very difficult to determine in advance, there is a good chance of arriving at the wrong answer; to solve the problem, you need to either "reduce the size of the haystack, or improve our procedure for evaluating candidate answer.")

[97] U.S. Secret Service Criminal SORN, *supra* note 84.

based on high quality information, which doesn't seem to be a provision from which one would want to exclude oneself. The Privacy Act Guidelines in fact recognize "the difficulty of establishing absolute standards of data quality", and "places the emphasis on assuring the quality of the record in terms of the use of the record in making decisions affecting the rights, benefits, entitlements, or opportunities… of the individual."[98] Subsection (e)(5) requires only that DHS perform quality checks on its records when adverse determinations about individuals are being made.

Interestingly, the DHS subagencies that claim general exemptions in SORNS also claim specific exemptions, even though the specific exemptions are encompassed by the claim to general exemptions. It is unclear why DHS would do this, unless it is fearful that its claims to general exemptions might be challenged.

Despite the fact that general exemptions are restricted by the Act to specific types of agencies and records, DHS has claimed general exemptions for subagencies that 1) don't appear to have the required functionality necessary for general exemptions to apply and 2) don't appear to hold records that meet the requirements of general exemptions. These include the U.S. Secret Service's Non-Criminal Investigation Information System of Records (whose SORN is effectively identical to the Secret Service's Criminal Investigation Information System of Records); Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection (ICEPIC) System; and the U.S. Customs and Border Protection (CBP) Automated Targeting System (ATS) System of Records. These subagencies do not all have the principal function of criminal law enforcement; the CBP and ICE are responsible for the enforcement of many kinds of

[98] Privacy Act Guidelines, *supra* note 33 at 28964.

laws.[99] It is clear in the language of the Privacy Act that records belonging to the U.S. Secret Service are not automatically presumed to fall under general exemptions; exemption (k)(3) explicitly categorizes Secret Service records "maintained in connection with providing protective services to the President of the United States" as qualified for specific exemptions.

Furthermore, the DHS systems of records analyzed herein do not necessarily satisfy any of the three Privacy Act record-type requirements for general exemptions. Most of the records in the Automated Targeting System (ATS) System of Records, for example, do not pertain to existing criminal investigations. They instead analyze data collected on individual travelers, whether or not there is a criminal investigation open on those individuals.

DHS is an agency composed of many subagencies, whose mandates vary from fighting terrorism to enforcing noncriminal immigration regulations and providing support in situations of national emergency. It appears from this short analysis that DHS subagencies reach for general exemptions where they might not be qualified for them.

Only one of the five DHS SORNs examined did not claim any exemptions: the SORN for FEMA's National Emergency Family Registry and Locator System System of Records. Notably, the information in this system differs in kind from the information included in the other systems—it is not maintained even remotely for law enforcement purposes, and DHS does not make this claim. But also notably, the FEMA SORN was

[99] It is not clear from caselaw what constitutes an agency that "performs as its principal function any activity pertaining to the enforcement of criminal laws" under (j)(2). Discussions of the relationship between statutory mandate and law enforcement activities have been limited for the most part to examining an agency's rationale for its investigation's relationship to its law enforcement duty—not to examining whether the agency is a criminal law enforcement agency to begin with. *See Doe v. F.B.I.*, 936 F.2d at 1354-1355.

issued in September, 2009, perhaps indicating a shift in DHS policy from claiming the same exemptions for all of its databases. However, the FEMA SORN provides for only one month of comments before the rule goes into effect, which does not encourage transparency. It also contains a large number of routine uses, expanding the dissemination of the information beyond the face of Privacy Act requirements. If this SORN does represent a shift in DHS policy on SORNs, it is not a policy of uniform respect for the Privacy Act.

ii. DHS Routine Use: Elimination of dissemination restrictions

Since effectively the only restrictions that remain after DHS's claimed exemptions in most of its SORNs are restrictions on the dissemination of gathered information, this paper now turns to the routine uses claimed by DHS. Routine uses refer to the disclosures of information outside of the agency or subagency that have been brought into the agency's uses so as to be exempt from criminal sanctions under the Privacy Act. Agencies also often publish routine use exceptions prior to, and therefore separate from, the publication of exemptions claimed, lessening the transparency function of SORNs.

Several routine uses are customarily claimed by agencies, and are not particularly problematic. These include: disclosure to DOJ or other Federal agencies for litigation purposes; disclosure to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains; disclosure to National Archives and Records Administration (NARA); disclosure for the purpose of audits and oversight; disclosure to contractors and their agents, subject to the restrictions of the Privacy Act; disclosure to other federal

agencies in the process of hiring an individual; and disclosure to the appropriate party, with restrictions, where the agency believes the security of information might have been compromised.[100] It is worth noting, because of the increasing use of private contractors by federal agencies, that when any agency contracts with a private contractor, its exemptions from the Privacy Act extend to that contractor as well. This is significant because in the case of most DHS agencies private contractors are removed from the scope of the Act's civil sanctions, and criminal sanctions relating to dissemination when the dissemination requirements are lessened by routine use exceptions.

DHS SORNs add a law enforcement routine use to the above.[101] Under subsection (b)(7) of the Privacy Act, agencies may disclose records to another agency for law enforcement purposes if the head of that agency or instrumentality has specifically requested the records in writing. Even the most restrictive DHS SORN, the FEMA SORN, adds to routine uses the disclosure of records to "an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority … where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law… and such disclosure is proper and consistent with the official duties of the person making the disclosure".[102] In other words, FEMA authorities may proactively contact other agencies with information from their records indicating potential legal violations of either civil or criminal law; they needn't wait for those agencies to contact them.

---

[100] *See, e.g.*, United States Secret Service, Criminal Investigation Information System of Records Notice, 73 FR 77729-02 (Dec. 19, 2008), 2008 WL 5262553 (F.R.) [herinafter U.S. Secret Service Crim SORN 2].
[101] The Department of Defense (DoD) Blanket Routine Uses includes a Law Enforcement routine use as well. 32 C.F.R. § 310 Appendix C (A).
[102] FEMA NEFR SORN, *supra* note 79.

The Privacy Act Guidelines do discuss the possibility of including law enforcement disclosures as routine uses. The Guidelines suggest, however, that these routine uses be limited to emanating from systems of records that are "law enforcement systems".[103] The Guidelines state that "[r]ecords in law enforcement systems may also be disclosed for law enforcement purposes when that disclosure has properly been established as a "routine use"".[104] The examples provided indicate that these routine uses were imagined as narrowly tailored to the originating agency's purpose: "e.g., statutorily authorized responses to properly made queries to the National Driver Register; transfer by a law enforcement agency of protective intelligence information to the Secret Service".[105] FEMA's expansion of use of its records to providing law enforcement tips to law enforcement agencies is beyond the imagined scope of exceptions to the dissemination requirement. It is also commonly employed, as will be seen in the DHHS routine use exceptions, below.

The FEMA type of law enforcement routine use, however, is still more confined than the routine uses applied to records held by other subagencies in DHS. ICE, for example, provides for disclosure as a routine use to Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental agencies "where DHS determines that the information would assist in the enforcement of domestic and foreign civil or criminal laws."[106] ICE also provides for routine use disclosure to federal, state, tribal, local, or foreign government agency or organization, or international organization "lawfully engaged in collecting law enforcement intelligence, whether civil or criminal"

---

[103] Privacy Act Guidelines, *supra* note 33 at 28955.
[104] *Id*.
[105] *Id*.
[106] Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection (ICEPIC) System, 73 FR 48226-01 (Aug. 18, 2008), 2008 WL 3821236 (F.R.) [hereinafter ICEPIC SORN 2].

to "enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence".[107] ICE is able, in other words, to widely disclose the records in ICEPIC not just when it suspects a violation of law, as in the FEMA SORN, but more broadly to aid in intelligence gathering or law enforcement internationally. This broad routine use, by comparison to another agency, is not included in the Department of Defense (DoD)'s Blanket Routine Uses.[108]

Similarly, CBP's ATS SORN allows routine use disclosure to federal, state, local, tribal, or foreign governmental agencies responsible for investigation or prosecuting or even just implementing statutes, regulations, or even licenses, "where CBP believes the information would assist enforcement of applicable civil or criminal laws".[109] Again, this is not equivalent to requiring CBP to suspect a violation of a specific law by a specific record. It allows CBP to share airplane passenger data with foreign governments or organizations merely to "assist enforcement" of "applicable" laws. CBP can also routinely disclose information to foreign government intelligence "where such use is to assist in anti-terrorism efforts", not just when CBP becomes aware of a threat or potential threat.[110]

Several DHS SORNs include a perhaps even more problematic routine use: the disclosure of information to third party individuals during an investigation. The ICEPIC SORN provides for such disclosure "to other individuals and organizations during the course of an investigation by DHS… when DHS deems that such disclosure is necessary

---

[107] *Id*.
[108] 32 C.F.R. § 310 Appendix C.
[109] U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 FR 43650-02 (Aug. 6, 2007), 2007 WL 2227240 (F.R.) (2007) [hereinafter CBP ATS SORN 2].
[110] *Id*.

to elicit information required to accomplish the purposes described".[111] Similarly, CBP's ATS SORN lists as a routine use disclosure to "third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation."[112] CBP does, however, condition such disclosure to nongovernmental third parties as performable only when "disclosure is appropriate in the proper performance of the official duties of the officer making the disclosure." By comparison, again, this routine use is not included in the Department of Defense (DoD)'s Blanket Routine Uses.[113]

The FEMA SORN for the National Emergency Family Registry and Locator System also includes an extremely broad category of routine use: disclosure to federal agencies, state, tribal, local governments, local law enforcement, and voluntary organizations that have an established disaster assistance program.[114] Broader than the law enforcement routine use, this effectively allows full dissemination of FEMA-held emergency information to anybody in the government, rather than within the agency only. Note that this disclosure is not contingent on the existence of an actual emergency, and is contingent on the existence of an established disaster assistance program only for voluntary organizations.

In summary, DHS agencies provide routine uses that expand the dissemination of information well outside of the scope of dissemination contemplated by the Privacy Act. Coupled with the exemptions claimed by DHS under (j)(2), this expansion effectively removes DHS agencies from under the umbrella of the Privacy Act.

---

[111] ICEPIC SORN 2, *supra* note lkj.
[112] ATS SORN, *supra* note **lkj.**
[113] 32 C.F.R. § 310 Appendix C.
[114] FEMA SORN, *supra* note **lkj.**

b. Department of Health and Human Services

The SORNs for the Department of Health and Human Services (DHHS) are both less uniform than DHS SORNs, and less extensive in their claims of exemptions. Some of these differences are attributable to a difference in the type of agencies and the type of records at hand: DHHS is not a criminal law enforcement agency, and its records are therefore not subject to general exemptions. Other differences, however, seem to be a function of differences in the scope of agency claims. DHHS agencies do claim routine use exemptions, but again the scope of the claims varies widely by agency, and the routine uses claimed are not nearly as broad as those claimed by DHS.

i. Exemptions: Far fewer exemptions claimed

Subagencies under the DHHS claim far fewer exemptions than DHS subagencies. Again, this is in large part because DHHS subagencies clearly do not qualify for general exemptions as a criminal law enforcement agency. However, even those that qualify for specific exemptions do not use SORNs to claim all available exemptions. This section tracks DHHS SORNs' use of exemptions chronologically.

The SORN for the Welfare Fraud Detection File,[115] published in 1982, claims no exemptions for the system of records, despite the fact that the system "has as its major function the identification of cases which through misrepresentation are on the welfare rolls illegally."[116] The fact that DHHS claims no exemptions for this system indicates that at least initially, special exemptions were conceived of as something an agency would take only when necessary, not as habit.

---

[115] 47 FR 45514-01, 1982 WL 190825 (F.R.) [hereinafter Welfare Fraud SORN].
[116] *Id*.

The SORN for Alcohol, Drug Abuse, and Mental Health Epidemiologic Data, issued by the Substance Abuse Mental Health Substance Agency (SAMHSA) in 1993, and again in 1999, claims no exemptions from the Privacy Act.[117]

The SORN for the Healthcare Integrity and Protection Data Bank (HIPDB)[118], which was published in 1999, claims effectively two exemptions, under the specific exemption law enforcement provision. 5 U.S.C. § 552a(k)(2). The HIPDB consists of records on health care practitioners and suppliers who are the subjects to final adverse actions, including criminal convictions, civil judgments, and actions by federal or state agencies. Despite the fact that the HIPDB includes records of criminal convictions, DHHS does not attempt to claim a criminal law enforcement exemption. Instead, HIPDB is exempted from the access and amendment provisions of the Privacy Act ((c)(3), (d)(1)-(4)) and the requirement that it publish agency procedures for access ((e)(4)(G) and (H)) as "investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section" under (k)(2).

The SORN for the National Disaster Medical System (NDMS) Patient Treatment and Tracking system[119], published in 2007, claims no exemptions from the system, despite the fact that the agency coordinates with DHS and DoD on these records, and shares the information with them. It does, however, claim a number of routine uses, outlined below.

ii. Routine Use: Narrower carve-outs from dissemination requirements

[117] 58 FR 68993-01, 1993 WL 537661 (F.R.) (1993), and 64 FR 2909-01, 1999 WL 15385 (F.R.) (1999) [hereinafter Alcohol Abuse SORN].
[118] 64 FR 7652-02 (Feb. 16, 1999), 1999 WL 67701 (F.R.) [hereinafter HIPDB SORN].
[119] 72 FR 35052-01 (June 26, 2007), 2007 WL 1812533 (F.R.) [hereinafter NDMS SORN].

Subagencies under the DHHS claim fewer and less expansive routine uses than DHS subagencies. Some agencies claim very few routine uses; others claim significantly more. It is particularly noticeable that the most recent DHHS SORN analyzed, which combines efforts with DHS agencies, more closely resembles the broad scope of routine use claims in DHS SORNs. This section tracks DHHS SORNs' routine uses chronologically.

The SORN for the Welfare Fraud Detection File, published in 1982, includes many of the standard routine uses seen to operate above.[120] The SORN includes the following fairly typical routine use disclosures: in the event of litigation; to a congressional office; for employment purposes, either to obtain documents or to inform another agency considering employment. The SORN also includes the following: disclosure to DOJ for advice on FOIA requests; disclosure to another agency when that agency has issued a subpoena; disclosure to contractors or agents; and disclosure to student volunteers.

The Welfare Fraud Detection File does include a law enforcement routine use. It should be noted, however, that the use is, like the FEMA SORN, limited to when the agency suspects a violation of law. When a record "indicates a violation or potential violation of law", the agency may disclose that record "to the appropriate agency, whether state or local". This also does not include international or multilateral organizations or legal systems, unlike the DHS law enforcement routine use.

The SORN for Alcohol, Drug Abuse, and Mental Health Epidemiologic Data, issued by the Substance Abuse and Mental Health Services Administration (SAMHSA)

---

[120] Welfare Fraud SORN, *supra* note 105.

in 1993, and again in 1999, claims four categories of routine uses. [121] Three are, again, fairly typical: to a congressional office, in the event of litigation, and pursuant to contract with a private firm. The fourth is disclosure to an agency or individual "for an evaluation purpose" under tight restrictions outlined in the SORN, and subject to a written statement of the recipient's understanding of, and willingness to abide by, those provisions. SAMHSA does not include a law enforcement routine use exception.

The SORN for the Healthcare Integrity and Protection Data Bank (HIPDB), published in 1999, claims only two categories of routine uses.[122] The first is similar to the employment routine use in the DHS SORNs: disclosure to "a health plan requesting data concerning a health care provider, supplier, or practitioner for the purposes of preventing fraud and abuse activities… and in the context of hiring or retaining providers… that are the subjects of reports". The second routine use claimed is more like a law enforcement routine use. Strikingly, however, it requires affirmative requests on the part of other government agencies requesting access to the records, rather than allowing DHHS to distribute such records to law enforcement agencies.[123]

The SORN for the National Disaster Medical System (NDMS) Patient Treatment and Tracking system, published in 2007, claims six routine uses.[124] These uses include disclosure to a member of Congress; disclosure to DOJ during litigation; and disclosure to agency contractors. They also include two routine uses specific to this system: to assist another agency to find its beneficiary and assess that beneficiary's "status", and to help a

---

[121] Alcohol Abuse SORN, *supra* note 107.
[122] HIPDB SORN, *supra* note 108.
[123] DHHS provides for disclosure to "[g]overnment agencies… requesting data concerning a health care provider, supplier or practitioner for the purposes of preventing fraud and abuse activities and/or improving the quality of patient care… This would include law enforcement investigations and other law enforcement activities." *Id*.
[124] NDMS SORN, *supra* note 109.

family member locate or determine the status of the patient. It is unclear whether the system allows for restrictions on, say, the location of patients by abusive spouses. The SORN also allows DHHS to disclose all information to DHS, DoD, and the Department of Veterans Affairs (VA). DHHS explains that "the medical treatment and evacuation of patients is a shared responsibility between these agencies and disclosure of health related information is necessary to adequately manage the overall care of the patient." Despite this explanation, the SORN provides for full disclosure, not disclosure conditioned restricted use to enabling the medical treatment and evacuation of patients, to DHS, DoD, and VA, with no further restrictions on how the respective agencies in turn use such information.

c. The Impact of SORNs

The result of agency use of SORNs is that while the Privacy Act still can, and does, provide substantial data protection in some federal agencies, it does little to regulate much of the information collected and kept by other agencies, such as DHS. This is disturbing because as agencies increasingly combine databases or make them accessible across agencies, the data maintenance and integrity requirements of the Privacy Act do not apply, despite the strong facial message of the statute.

This has multiple implications for U.S. citizens and LPRs. First, sharing data with law enforcement agencies without suspecting a specific violation of law likely creates a flood of potentially irrelevant information that must be processed by the receiving agencies. That processing includes determining the quality and relevance of the data, placing a huge burden on the receiving agency. Second, eased maintenance requirements obtained through Privacy Act exemptions mean that collected data often need not be

"relevant and necessary" to the agency's purpose, and that data need not meet a certain level of quality before determinations can be made based on it. Useless and inaccurate data is likely to be included as a result, and eased restrictions on quality of data create added difficulty in determining what information is actually useful. Both of these changes again make it more difficult, not easier, for law enforcement agencies to do their jobs.

Third, there are obvious privacy problems with allowing any information that enters the federal system to be routinely disclosed to other federal agencies, state government, foreign governments, and even third parties without sanctions for misuse or inaccuracy.

Proposals for Change

This paper proposes a tiered set of solutions for the problems raised above, addressing both courts and Congress. The Fair Information Practices articulated in the Privacy Act are admirable and potentially functional, and it is conceivable that with some tweaks, much of government data treatment can be brought back under the provisions of the Act without requiring new legislation. This paper therefore proposes several solutions that need not require major new legislation. In the absence of such solutions, however, this paper proposes that Congress take up the mandate left hanging by provision (j)(2) at the time the Privacy Act was enacted: create federal privacy legislation that explicitly applies modified Fair Information Practices to federal criminal law enforcement agencies, including information gathered explicitly for the purposes of criminal investigations.

a. Courts

There are three interpretive areas in which courts could greatly impact the use of SORNs by federal agencies. The first two concern the scope of the criminal law enforcement agency exemption; the third concerns the scope of routine use.

Courts need to both define what constitutes a criminal law enforcement agency, and determine whether such agencies can exempt themselves from the Privacy Act for material obtained by broad surveillance. This paper proposes that courts define "criminal law enforcement agency" narrowly, limiting its scope to agencies or subagencies actually primarily engaged in criminal law enforcement activity, regardless of the role of the parent agency. For example, DHS has been routinely exempting many of its subagencies that do not appear to be criminal law enforcement agencies from Privacy Act provisions. A narrower definition of "criminal law enforcement agency" would preclude such subagencies from claiming the broadest Privacy Act exemptions. This interpretation would be in keeping with the principles behind the criminal law enforcement agency exemption. The security and intelligence-gathering justifications for removing true criminal law enforcement agencies from the scope of most of the Privacy Act does not apply to subagencies that don't primarily serve a criminal law enforcement function.

Courts also need to resolve conflicting case law on whether criminal law enforcement agencies can exempt themselves from Privacy Act provisions for material obtained by broad surveillance or data-gathering not tied to specific investigations. This paper proposes that courts should resolve this question to exclude from general exemptions any criminal law enforcement records on individuals that are not tied to a specific criminal investigation. In doing so, courts would bring sweeping intelligence gathering back into the scope of the Privacy Act and allow innocent individuals access to

the records kept on them. Where surveillance is tied to a specific criminal investigation, courts may appropriately leave such information within the exemptions to the Act.

Finally, courts should address the scope of the routine use provisions. Courts should analyze the routine use provisions with a view to the purposes of the Privacy Act as a whole, and articulate restrictions on how widely an agency can remove itself from the act's fundamental dissemination provisions. Regardless of whether courts end up addressing the scope of law enforcement exemptions, restricting the scope of routine use would at least ensure that data not be over-disseminated.

b. Congress

Congress can either act in small increments to alter and improve the existing Privacy Act, or create new legislation entirely. This paper proposes that Congress enact new, but similar, legislation addressing criminal law enforcement agencies conducting criminal investigations. In the absence of such legislation, however, Congress can similarly narrow the exemptions and routine uses of the Privacy Act to broaden the scope of existing legislation.

Congress more narrowly as to what constitutes a criminal law enforcement agency, reaffirming that subagencies that do not primarily deal with criminal law should not be subject to the criminal law enforcement exemption. Congress should also address concerns about data quality by altering the Act to ensure that even criminal law enforcement agencies must maintain all records with "accuracy, relevance, timeliness, and completeness".[125] Congress also needs to address the scope of routine use provisions with more precision, limiting agencies' abilities to take themselves out of dissemination restrictions entirely.

[125] 5 U.S.C. 552a(e)(5).

More pressingly, however, Congress should create federal privacy legislation that explicitly applies modified Fair Information Practices to federal criminal law enforcement agencies, including information gathered explicitly for the purposes of criminal investigations. This legislation should certainly exclude requirements that individuals be able to access files held on them in the course of a criminal investigation; it should, however, create mandated processes for individuals to participate in the correction of faulty information held on them by such agencies, and should require quality assurance standards, supported by sanctions, for all data held. These practices benefit both the agencies themselves, by ensuring that data is relevant and of high quality, and individuals, by protecting their privacy from broad surveillance measures and inefficient bureaucracy and inaccurate processing.

Conclusion

The Privacy Act was meant to serve as the legal articulation of Fair Information Practices (FIPs) for federal agencies. As part of that policy, agencies are required to publish notice of the creation and modification of systems of records, and any exemptions claimed. Agencies have used these System of Records Notices (SORNs), however, to both loosen Privacy Act restrictions on the dissemination of information and to exempt themselves from substantial portions of the Privacy Act. In an age of increased digitalization and sharing of information in the name of federal law enforcement, Congress and courts need to make a decision about the scope of the Privacy Act and its exemptions.[126] Otherwise, the Privacy Act, which could be a clear statement of U.S.

[126] Kenneth A. Bramburger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. Chi. L. Rev. 75-76 (2008) (observing that "the digital collection of personally identifiable information renders that data subject to the immense search and aggregation powers of technology systems,

government privacy practices, will remain effectively defunct, based on agency choice alone.

increases the capacity for repurposing and reuse, and provides increasingly attractive targets to hackers bent on misuse… [raising] serious concerns about a surveillance capacity that can erode personal privacy").